Notre Dame Journal of Law, Ethics & Public Policy

Volume 31 | Issue 1 Article 4

2017

Investigative Journalism and Counter Terrorism Laws

Clive Walker
University of Leeds

Follow this and additional works at: http://scholarship.law.nd.edu/ndjlepp

 Part of the Legal Ethics and Professional Responsibility Commons, National Security Law Commons, and the Rule of Law Commons

Recommended Citation
Clive Walker, *Investigative Journalism and Counter Terrorism Laws*, 31 Notre Dame J.L. Ethics & Pub. Pol'y 129 (2017).
Available at: http://scholarship.law.nd.edu/ndjlepp/vol31/iss1/4

This Article is brought to you for free and open access by the Notre Dame Journal of Law, Ethics & Public Policy at NDLScholarship. It has been accepted for inclusion in Notre Dame Journal of Law, Ethics & Public Policy by an authorized editor of NDLScholarship. For more information, please contact lawdr@nd.edu.

INVESTIGATIVE JOURNALISM AND COUNTER TERRORISM LAWS

CLIVE WALKER*

ABSTRACT

Since terrorism is now perceived as a primary and pervasive threat to state security, many states have adopted broad legal definitions of "terrorism" and, upon that basis, have enacted correspondingly expansive policing powers and criminal offences. As a dramatic instance of how these approaches, which affect major Western jurisdictions such as the U.S. and U.K., this paper will focus on the paradigm case of David Miranda. In August 2013, Miranda was transporting computer materials (including files from security agencies) supplied by Edward Snowden, a former contractor with the U.S. National Security Agency, to journalist Glenn Greenwald to assist ongoing disclosures in The Guardian and other publications. The materials were seized during an examination and detention of Miranda while he was transiting through Heathrow Airport. The journalists viewed their mission as one of ethical disclosure in the public interest of a vast web of governmental surveillance programmes. However, the U.K. Security Service (MI5) contended that Miranda was involved in 'terrorism' (as defined in the U.K. Terrorism Act 2000, section 1) because his mission sought to influence the government by promoting a political or ideological cause. The allegation was that disclosure of the data to a hostile state (Russia), or to terrorists, might imperil the identities of secret agents or the methods used for electronic surveillance of terrorists. Thus, the material fell into the realms of terrorism. On these grounds, Miranda was held under special detention powers relating to counter-terrorism at borders, and the materials were seized. Similar arguments were then used to persuade the editor of The Guardian to destroy other materials held in the newspaper offices. In a subsequent court review, Miranda v Secretary of State for the Home Department, the meaning of who qualifies as a 'terrorist' and whether the journalistic activity being pursued by Miranda, Greenwald, and others should be excluded from that depiction was explored. This paper seeks to reflect upon the complex linkages between journalistic activities and the label of 'terrorism,' which is becoming a primary threat to investigative journalism in the contemporary world. It will require reflection upon the conceptual nature of terrorism and journalism in a setting of ethics, public policy, and law.

* Professor Emeritus of Criminal Justice Studies, School of Law, University of Leeds, Leeds LS2 9JT, United Kingdom, law6cw@leeds.ac.uk. An earlier version of this paper was presented at the conference on *Freedom of Information, and Governmental Transparency, in the Open Government Era*, University Paris 1 Panthéon-Sorbonne, 10 & 11 March 2015, Paris, France.

I. INTRODUCTION

The development and exposure of public policy requires champions. Lawyers and politicians may fondly believe that they are the self-appointed champions, however, journalists have at least an equal claim to a leadership role. They may be viewed as unencumbered by the special interests of their client or their political allegiance. More positively, journalists have a special public interest role to play in informing the public.

The European Court of Human Rights has long been keen to underline the press's role as champions of informing the public about public policy issues, including with regard to reporting about terrorism. In *Castells v. Spain, it was suggested that:*

> Freedom of the press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes of their political leaders. In particular, it gives politicians the opportunity to reflect and comment on the preoccupations of public opinion; it thus enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society.[1]

The conferment of a special press role was extended in *Jersild v. Denmark*, where the European Court of Human Rights accepted that "[a]lthough formulated primarily with regard to the print media, these principles doubtless apply also to the audio-visual media."[2] One may also find in the jurisprudence of the European Court of Human Rights more specific approbation of the role of investigative journalism through its attraction of an especially high level of protection in principle, both against claims to the disclosure of sources[3] and challenges by way of libel suit.[4]

As applied to journalistic coverage of terrorism, the European Court of Human Rights has considered many applications relating to the reporting of the statements of terrorists or persons sympathetic to terrorist causes. Civil or criminal actions against the media for reports or discussion of such statements have been closely dissected by the Court for any sign of the endorsement or encouragement of violence which will divest the journalist of any protection from free speech rights under Article 10 of the European Convention on Human Rights.[5] In

1. Castells v. Spain, 236 Eur. Ct. H.R. (ser. A) at 43 (1992).

2. Jersild v. Denmark, 298 Eur. Ct. H.R. (ser. A) at 31 (1995).

3. *See* Goodwin v. United Kingdom, 1996-II Eur. Ct. H.R. 483; Nordisk Film & TV A/S v. Denmark, App. No. 40485/02 Eur. Ct. H.R. (2005); Voskuil v. Netherlands, App. No. 64752/01 Eur. Ct. H.R. (2007); Fin. Times Ltd. v. United Kingdom, App. No. 821/03 Eur. Ct. H.R. (2009); Sanoma Uitgevers B.V. v. Netherlands, App. No. 38224/03 Eur. Ct. H.R. (2010); Telegraaf Media Nederland Landelijke Media B.V. v. Netherlands, App. No. 39315/06 Eur. Ct. H.R. (2012).

4. *See* Cumpănă & Mazăre v. Romania, 2004-XI Eur. Ct. H.R. 63, 96; Mosley v. United Kingdom, App. No. 48009/08 Eur. Ct. H.R. 129 (2011).

5. *See generally* CLIVE WALKER, BLACKSTONE'S GUIDE TO THE ANTI-TERRORISM LEGISLATION 39–82 (3d ed. 2014).

Zana v. Turkey,[6] the applicant's statement of sympathy for the Partiya Karkerên Kurdistanê (Kurdistan Workers' Party, known as the "PKK") was regarded as likely to exacerbate an already violent situation and so was unprotected by Article 10, even though the applicant was a mayor in the region. In *Gündüz v. Turkey*,[7] a call upon supporters to produce "one brave man among the Muslims to plant a dagger in their soft underbelly and run them through twice with a bayonet" was unprotected, as was a cartoon in praise of the September 11 attacks published in the Basque country in *Leroy v. France*.[8] Thus,

> forms of identification with a terrorist organisation, and especially apologia for such an organisation, may be regarded as a manifestation of support for terrorism and an incitement to violence and hatred. Similarly, the Court accepts that to disseminate messages praising the perpetrator of an attack, to denigrate the victims of an attack, to raise money for terrorist organisations, or to engage in other similar conduct, may constitute acts of incitement to terrorist violence . . . .[9]

But where, as in *Arslan v. Turkey*,[10] the Court was sure that the words used did not constitute an incitement to violence, it defended statements; in this case those in a book, which alleged that the Turkish state oppressed the Kurds and so, explained the consequent "resistance" and "Kurdish intifada." As made clear in *Gerger v. Turkey*,[11] words such as "resistance", "struggle", and "liberation" do not necessarily constitute an incitement to violence. The more neutral reportage of declarations or interviews of terrorist representatives by media professionals will also tend to attract the protection of the Court, as established in *Sürek and Özdemir v. Turkey*,[12] and latitude is also given to artistic and academic

6. Zana v. Turkey, 1997-VII Eur. Ct. H.R. *See also* Sürek v. Turkey (No. 1), 1999-IV Eur. Ct. H.R. 353; Sürek v. Turkey (No. 3), App. No. 24735/94 Eur. Ct. H.R. (1999); Falakaoglu & Saygili v. Turkey (No. 3), App. No. 22147/02, 24972/03 Eur. Ct. H.R. (2007).

7. Gündüz v. Turkey, 2003-XI Eur. Ct. H.R. 435, 439.

8. Leroy v. France, App. No. 36109/03 Eur. Ct. H.R. (2008).

9. Güler & Uğur v. Turkey, App. No. 31706/10, 33088/10 Eur. Ct. H.R. 52 (2014).

10. Arslan v. Turkey, App. No. 23462/94 Eur. Ct. H.R. 17 (1999); *see also* Ceylan v. Turkey, App. No. 23556/94 Eur. Ct. H.R. (1999); Erdoğdu v. Turkey, App. No. 25723/94 Eur. Ct. H.R. (2000).

11. Gerger v. Turkey, App. No. 24919/94 Eur. Ct. H.R. 50 (1999); *see also* Erdoğdu and İnce v. Turkey, App. No. 25067/94, 25068/94 Eur. Ct. H.R. (1999); Okçuoglu v. Turkey, App. No. 24246/94 Eur. Ct. H.R. (1999); Polat v. Turkey, App. No. 23500/94 Eur. Ct. H.R. (1999).

12. Özdemir v. Turkey, App. No. 23927/94, 24277/94 Eur. Ct. H.R (1999); *see also* Sürek v. Turkey (No. 2), App. No. 24122/94 Eur. Ct. H.R. (1999); Sürek v. Turkey (No. 4), App. No. 24762/94 Eur. Ct. H.R. (1999); Önal v. Turkey, App. No. 41445/04, 41453/04 Eur. Ct. H.R. (2012); Belek v. Turkey, App. No. 36827/06, 36828/06, 36829/06 Eur. Ct. H.R. (2012); Bayar v. Turkey, App. No. 39690/06 Eur. Ct. H.R. (2014); Bayar and Gürbüz v. Turkey (No.2), App. No. 33037/07 Eur. Ct. H.R. (2015); Öner and Türk v. Turkey, App. No. 51962/12 Eur. Ct. H.R. (2015); Belek and Velioğlu v. Turkey, App. No. 44227/04 Eur. Ct. H.R. (2015); Müdür Duman v. Turkey, App. No.15450/03 Eur. Ct. H.R. (2015).

speech.[13] This European jurisprudence has not stopped several European jurisdictions from enacting criminal offences against the direct or indirect incitement of terrorism, and other international law standard-setting encourages these measures.[14] An example is section 1 of the UK's Terrorism Act 2006,[15] which has been upheld as consistent with Article 10 by the English courts.[16]

The focus in this paper is not so much on the publication of reports about terrorism but on investigations into terrorism by journalists in which they seek to bring new, hidden information to the attention of the public. Attention was drawn to this theme by the case of David Miranda in 2013. Miranda was detained as a suspected terrorist at Heathrow Airport for the possession of materials supplied from Edward Snowden, materials being transported from Russia to Brazil for journalistic purposes. This episode, which is considered below, raised an acute dispute as to whether Miranda should primarily be treated as a journalist or as a terrorist. However, this paper addresses a wider issue than the precise circumstances of the Miranda case, namely, how investigative journalism has been affected by the context of terrorism. For these purposes, most attention will be paid to the laws in the United Kingdom, since that jurisdiction has long been the most active and influential designer of counter-terrorism legislation.[17]

The phenomenon of contemporary terrorism works in two ways, which are inimical to journalism. First, the stance of terrorists towards journalists seems to have become much more hostile. In recent times, journalists have become targets rather than witnesses or messengers. One early example of this trend was the killing of Daniel Pearl in Pakistan in 2002.[18] More recent illustrations of the targeting of journalists involve the murder of *Charlie Hebdo* journalists in Paris on 7 January

13. *See* Başkaya and Okçuoğlu v. Turkey, App. No. 23536/94, 24408/94 Eur. Ct. H.R. (1999); Karataş v. Turkey, App. No. 23168/94 Eur. Ct. H.R. (1999).

14. *See* S.C. Res. 1624 (Sept. 14, 2005); Council of Europe, Convention on the Prevention of Terrorism art. 5, May 16, 2005, C.E.T.S. No. 196; Council Framework Decision 2008/919/JHA, art. 3, 2008 O.J. (L 330) 21 (EU).

15. *See* Adrian Hunt, *Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism*, 2007 CRIM. L. REV. 441 (2007); Ellen Parker, *Implementation of the UK Terrorism Act 2006—The Relationship Between Counterterrorism Law, Free Speech, and the Muslim Community in the United Kingdom Versus the United States*, 21 EMORY INT'L L. REV. 711 (2007); Eric Barendt, *Incitement to, and Glorification of, Terrorism*, *in* EXTREME SPEECH AND DEMOCRACY 445 (Ivan Hare and James Weinstein eds., 2009); Tufyal Choudhury, *The Terrorism Act 2006: Discouraging Terrorism*, *in* EXTREME SPEECH AND DEMOCRACY, at 463; S. Chehani Ekaratne, *Redundant Restriction: The U.K.'s Offense of Glorifying Terrorism*, 23 HARV. HUM. RTS. J. 205 (2010); Clive Walker, *Militant Speech About Terrorism in a Smart Militant Democracy*, 80 MISS. L.J. 1395 (2011). *See generally* WALKER, *supra* note 5, at 39–82.

16. R v. Faraz [2012] EWCA (Crim) 2820 (UK); R v. Gul [2013] UKSC 64; Iqbal v. R [2014] EWCA (Crim) 2650 (UK).

17. *See* Clive Walker, *Terrorism and Criminal Justice: Past, Present and Future*, 2004 CRIM. L. REV. 311 (2004); KENT ROACH, THE 9/11 EFFECT: COMPARATIVE COUNTER-TERRORISM (2011).

18. Ahmad Omar Saeed Sheikh was sentenced to death in Hyderabad in 2002. Rory McCarthy, *Underworld where terror and security meet*, GUARDIAN (July 16, 2002, 3:30 AM), http://www.theguardian.com/world/2002/jul/16/pakistan.rorymccarthy; Daniel McGrory, *CIA Paid Pakistan for terror suspects*, AUSTRALIAN (Sept. 26, 2006, 12:00 AM),

2015[19] and killings by the Islamic State and its affiliates in Syria.[20] Reasons for this growing hostility may include not only the vehemence of the rejection by extreme Islamist groups of modernist cultures, but also, paradoxically, their embrace of new media technologies. The internet affords several advantages to terrorists. Compared to print media, the internet is harder to control and restrict, has better cross-jurisdictional reach, and has lower running costs.[21] Furthermore, the Internet means that terrorists are no longer wholly reliant on the established—and often Western-controlled—mass media to act as carriers and intermediaries, thereby allowing them to attain otherwise unattainable prominence, explicitness, and meaning for their ideology and violent activities.[22] Thus, the internet now presents terrorists, whether mass movements or lone actors, with increased opportunities to propagate globally their own interpretations and messages,[23] and so jihadis and their online fans—"jihobbyists"[24]—increasingly have greater recourse to mainstream social media platforms.[25] For example, Al-Qa'ida in the Arabian Peninsula's online *Inspire* publication has been viewed as highly successful.[26] Now, Islamic State and their online supporters have proven themselves to be adept and prolific producers and dissemina-

---

http://www.theaustralian.com.au/news/world/cia-paid-pakistan-for-terror-suspects/story-e6frg6so-1111112268186.

19. *Police et Justice*, LE MONDE, http://www.lemonde.fr/attaque-contre-charlie-hebdo/ (last visited Feb. 18, 2016).

20. Prominent recent examples include the killings of James Foley (2014), Steven Sotloff (2014), Kenji Goto (2015), and Ruqia Hassan (2015). For global statistics of killings of journalists since 1992, *see Journalists Killed Since 1992*, COMM. TO PROTECT JOURNALISTS, https://www.cpj.org/killed/ (last visited Feb. 18, 2016).

21. Clive Walker & Maura Conway, *Online Terrorism and Online Laws*, 8 DYNAMICS ASYMMETRIC CONFLICT 156 (2015).

22. *See* SUSAN L. CARRUTHERS, THE MEDIA AT WAR: COMMUNICATION AND CONFLICT IN THE TWENTIETH CENTURY 170 (2000). These media roles sometimes resulted in threats of prosecution either for withholding information or for "apology" of terrorism. *See also* CLIVE WALKER, TERRORISM AND THE LAW 341–86 (2011).

23. *See* Maura Conway, *Cybercortical Warfare: Hizbollah's Internet Strategy*, *in* THE INTERNET AND POLITICS: CITIZENS, VOTERS AND ACTIVISTS 90 (Sarah Oates et al. eds., 2005); Maura Conway, *Terrorist Web Sites: Their Contents, Functioning, and Effectiveness*, *in* MEDIA AND CONFLICT IN THE TWENTY-FIRST CENTURY 185 (Philip Seib ed., 2005); Kelly Damphousse, *The Dark Side of the Web: Terrorists' Use of the Internet*, *in* CRIMES OF THE INTERNET 573 (Frank Schmalleger & Michael Pittaro eds., 2008); GABRIEL WEIMANN, NEW TERRORISM AND NEW MEDIA 2 (2014), https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf.

24. JARRET M. BRACHMAN, GLOBAL JIHADISM: THEORY AND PRACTICE 19 (2009). For Irish Republican internet usages, *see* Ross Frenett and M.L.R. Smith, *IRA 2.0: Continuing the Long War—Analyzing the Factors Behind Anti-GFA Violence*, 24 TERRORISM & POL. VIOLENCE 375 (2012). For right-wing groups, *see* GERMAN FED. OFFICE FOR THE PROT. OF THE CONSTITUTION, RIGHT-WING EXTREMISTS AND THEIR INTERNET PRESENCE (2013).

25. AARON Y. ZELIN, NEW AM. FOUND., THE STATE OF GLOBAL JIHAD ONLINE: A QUALITATIVE, QUANTITATIVE, AND CROSS-LINGUAL ANALYSIS (2013), http://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20130201-NewAmericaFoundation.pdf.

26. *See* Anthony F. Lemieux et al., *Inspire Magazine: A Critical Analysis of Its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model*, 26 TERRORISM & POL. VIOLENCE 354 (2014).

tors of digital content, especially through their *Dabiq* bulletins.[27] This growth of online content from terrorist groups and its potential attractiveness to, and resonance with, discontented "digital natives"—young people who have grown up with the internet—have become causes of official apprehension and legislative development throughout Europe[28] and globally. Therefore, the United Nations Security Council Resolution 2178—addressing the growing issue of foreign terrorist fighters—"urges Member States, in this context, to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law."[29]

It is dangerous enough to suffer potential attacks from terrorism, but the particular focus of this paper is directed towards the growing attacks on journalism from the state in pursuit of counter-terrorism. This counter-terrorism threat to journalism emerges in the form of a three-pronged attack.

First, there is the criminalization of journalistic activities by which the process of obtaining information and distilling it into news stories becomes depicted as a terrorist threat to the state. The first part of the paper considers the prime example of David Miranda.

Second, there is the demand for information generated by the activities of journalism. In this way, journalism is coerced into serving state interests, even if contrary to the journalistic ethics on the basis of which the information was amassed. This state capture of journalistic information may involve the more voluntary trading of information through on-going police-media cooperative relationships, but the interest of this paper lies in more coercive approaches. These will involve demands backed by legal sanctions, such as criminal offences or contempt of court, in reaction to police knowledge or suspicions that journalists possess potentially useful data.

Third, and perhaps most insidious of all, there may arise a demand for proactive information-giving from the media to the security authorities. In the United Kingdom, there is, again, an element of criminal coercion through anti-terrorism laws that is not common elsewhere in the Western world. This imposed duty of the media to provide information proactively without demand has become broader and shriller.

27. *See* Haroro J. Ingram, *Three Traits of the Islamic State's Information Warfare*, 159 RUSI J. 4 (2014); Jytte Klausen, *Tweeting the* Jihad*: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, 38 STUD. CONFLICT & TERRORISM 1 (2015).

28. *See* Eur. Consult. Ass., *Foreign Fighters and Returnees*, Doc. No. 14160/14 (2014); *Commission Proposal for a Directive of the European Parliament and of the Council on Combatting Terrorism and Replacing Council Framework Decision 2002/475/JHA on Combatting Terrorism*, at art. 5, COM (2015) 625 final (Dec. 2, 2015); Council of Europe, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Oct. 22, 2015, C.E.T.S. No. 127.

29. U.N. Security Council, Res. 2178, at Art. 17 (Sept. 14, 2014).

Proactive information transfer is also being encouraged on a more consensual basis, as revealed by Edward Snowden.

Having explored each of these three areas of challenge, the following part of the paper will analyse why these trends are occurring. Several suggested causes are mentioned. Some relate to the nature of terrorism and counter-terrorism. Some relate to the nature of the media. The analysis will be followed by some conclusions and the appropriate reactions.

II. Criminalisation of Journalistic Activities

The criminalisation of journalistic activities arises from the official apprehension that investigative journalism might pose a threat to state security. By way of evidence of current attitudes, it is instructive to refer to the Joint Services Publication 440, United Kingdom Ministry of Defence, a restricted security manual devised in 2001 and later revealed by Wikileaks.[30] It lists investigative journalists as a "non-traditional threat" to security whose activities are to be guarded against in the same way as foreign intelligence services and subversive or terrorist organizations.[31]

This perception is not new. Several prosecutions have been mounted against investigative journalists under UK official secrets legislation.[32] Prominent examples in the modern era[33] have included: *R. v. Cairns, Aitken and Roberts* in 1971, concerning a military assessment of the Biafran war;[34] and *R. v. Aubrey, Berry and Campbell* in 1978, concerning army signals intelligence.[35] In a case involving *The Guardian*[36] in

30. *UK MoD Manual of Security Volumes 1, 2 and 3 Issue 2, JSP-440, Restricted, 2389 pages, 2001*, WikiLeaks, https://wikileaks.org/wiki/UK_MoD_Manual_of_Security_Volumes_1,_2_and_3_Issue_2,_JSP-440,_RESTRICTED,_2389_pages,_2001 (last visited Apr. 12, 2016).

31. For the published assessment of security threats, *see* Cabinet Office, Cm. 7953, A Strong Britain in an Age of Uncertainty: The National Security Strategy (2010), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf; Cabinet Office, Cm. 9161, National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom 62 (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (promoting "free media" is an objective rather than a threat).

32. Most were brought under the Official Secrets Act 1911, 1 & 2 Geo. 5 c. 28, § 2 (UK), which was repealed and replaced by the Official Secrets Act 1989, c. 6 (UK). Home Office, Cmnd. 5104, Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972); Home Office, Cmnd. 7285, Reform of Section 2 of the Official Secrets Act 1911 (1978); Home Office, Cm. 408, Reform of Section 2 of the Official Secrets Act 1911 (1988).

33. *See also R v. Frederick Henry Budgen*, Times, July 15, 1932, at 4; *R v. Frederick Henry Budgen*, Times, Aug. 13, 1932, at 5; Joseph Jaconelli, *Wills as Public Documents—Privacy and Property Rights*, 71 Cambridge L.J. 147, 153–54 (2012); Compton Mackenzie, My Life and Times: Octave Seven, 1931–38 (1968).

34. *See R. v. Cairns, Aitken and Roberts*, Times, Feb. 4, 1971, at 1, 2, 15; Jonathan Aitken, Officially Secret (1971).

35. *See* Duncan Campbell, *Official Secrecy and British Libertarianism*, 16 Socialist Reg. 75 (1979); *see also* Crispin Aubrey, Who's Watching You? Britain's Security Services and the Official Secrets Act (1981); Geoffrey Robertson, The Justice Game (1999).

2011, the Metropolitan Police began proceedings under official secrecy legislation to force that newspaper to reveal how journalists had obtained information that the mobile phone of a murder victim (Milly Dowler) had been hacked. Consent of the Director of Public Prosecutions to prosecute *The Guardian* was not forthcoming, but sufficient evidence was amassed to bring proceedings against dozens of journalists, mainly from the *News of the World* newspaper—which was shut down in 2011 because of its scandalous behaviour—for illegal telephone interceptions and other offences.[37]

The danger of the criminalisation of journalists in connection with their reporting of terrorism lurks not only in the breadth of information which a government might view as useful to terrorism but also in what is counted as "terrorism." Amongst the special offences of greatest threat to journalism in the United Kingdom include section 58—possession of information useful to terrorism—and section 58A—eliciting, publishing, or communicating information about members of the security forces of a kind useful for terrorism such as by taking photographs—of Terrorism Act 2000, and the offence of attending training sites under section 8 of the Terrorism Act 2006.[38]

The most prominent recent illustration is, as mentioned earlier, the case of David Miranda. Miranda was not charged with any offence, but the portrayal of him—and his colleagues—as suspected terrorists opened up special policing powers and raised the possibility of journalists being charged with special terrorism-related offences. In *Miranda v. Secretary of State for the Home Department and the Commissioner of the Police of the Metropolis*,[39] the facts were that David Miranda was transporting computer materials from Berlin—including files from the Government Communications Headquarters ("GCHQ")—supplied by Edward Snowden, a former contractor with the U.S. National Security Agency ("NSA"). The materials had been supplied by journalist Laura Poitras in Berlin and were being transported to journalist Glenn Greenwald in Rio de Janeiro to assist with ongoing disclosures in *The Guardian* about GCHQ and the NSA.[40] The materials were seized during an examina-

36. *See* Michael Zander, *Dropping the Case*, 175 JUST. PEACE 573 (2011).

37. *See* BRIAN LEVESON, 1 AN INQUIRY INTO THE CULTURE, PRACTICES AND ETHICS OF THE PRESS (2012), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/270939/0780_i.pdf; R v. Coulson and Kuttner [2013] EWCA (Crim) 1026 (UK); *Crown Prosecution Service Re-review of Operation Elveden—Statement from the Director of Public Prosecutions*, CROWN PROSECUTION SERV. (Apr. 17, 2015), http://www.cps.gov.uk/news/latest_news/crown_prosecution_service_re_review_of_operation_elveden/index.html; *Statement from the Crown Prosecution Service: No Further Action to Be Taken in Operations Weeting or Golding*, CROWN PROSECUTION SERV. (Dec. 11, 2015), http://www.cps.gov.uk/news/latest_news/no_further_action_to_be_taken_in_operations_weeting_or_golding/.

38. *See* WALKER, *supra* note 5, at 181–210.

39. Miranda v. Sec'y of State of Home Dep't [2016] EWCA Civ 6 (UK); *see* Michael Zander, *Schedule 7 of the Terrorism Act 2000*, 178 CRIM. L. & JUST. WKLY. 151 (2014).

40. *Detained in the U.S.: Filmmaker Laura Poitras Held, Questioned Some 40 Times at U.S. Airports*, DEMOCRACY NOW! (Apr. 20, 2012), http://www.democracynow.org/2012/4/20/detained_in_the_us_filmmaker_laura (reporting that Poitras has been repeatedly detained and searched at U.S. airports); *see also* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); TRANSPARENT

tion and detention—for nine hours—of Miranda while he was transiting through Heathrow Airport in 2013.[41]

The powers that were invoked were part of the port and border control provisions under Part V and Schedule 7 of the Terrorism Act 2000.[42] Their purpose is to disrupt possible terrorist planning and logistics and also to gather intelligence. The controls also deter attacks on the travel facilities and on aircraft. Examining officers—who are mainly police officers—may question persons under Schedule 7, paragraph 1, for the purpose of determining whether they appear to be a "terrorist" within the Terrorism Act 2000, section 40(1)(b).[43] Reflecting the "all-risks" nature of these powers,[44] examining officers may exercise their powers whether or not they have suspicion against any individual—paragraph 2. In this way, the "copper's nose"[45] may guide application. Some interventions will be based on intelligence, perhaps related to destination, behavioural signals, or on documentary irregularities.[46] However, the use of examinations for extraneous purposes, such as to build the case for the issuance of an executive order, is not permitted—a limitation sustained in *CC v Commissioner of Police for the Metropolis*.[47] At the same time, that case confirms the following features: that the basis for intervention can be intuition; that the powers can be applied against someone already suspect in order to determine further details of involvement; and that examinations can continue even if initial indications of terrorism are negative.[48] A requirement of

---

LIVES: SURVEILLANCE IN CANADA (Colin J. Bennett et al. eds., 2014); BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE (2015).

41. *Miranda*,[2016] EWCA Civ 6 (UK).

42. *See* Terrorism Act 2000, c. 11, §53, sch.7 (UK); The Special Immigration Appeals Commission (Procedure) Rules 2003, SI 2013/1034, arts. 47–49 (UK). For the U.S. legal position, *see* Klayman v. Obama, 957 F. Supp. 2d 1 (D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015), *remanded to* 805 F.3d 1148 (D.C. Cir. 2015); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part and vacated in part*, 785 F.3d 787 (2d Cir. 2015); LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2013); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), *available at* http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf; PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 UK OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014), *available at* http://www.pclob.gov/Library/702-Report-2.pdf; CLIVE P. WALKER, BLACKSTONE'S GUIDE TO THE ANTI-TERRORISM LEGISLATION (3d ed. 2014).

43. *See also* CLIVE P. WALKER, THE PREVENTION OF TERRORISM IN BRITISH LAW 214 (2d ed. 1992).

44. *See* Clive P. Walker, *Neighbor Terrorism and the All-Risks Policing of Terrorism*, 3 J. NAT'L SECURITY L. & POL'Y 121, 123 (2009).

45. LORD CARLILE OF BERRIEW, REPORT ON THE OPERATION IN 2006 OF THE TERRORISM ACT 2000, 33 (2007).

46. *See* DAVID ANDERSON, THE TERRORISM ACTS IN 2011: REPORT OF THE INDEPENDENT REVIEWER ON THE OPERATION OF THE TERRORISM ACT 2000 AND PART 1 OF THE TERRORISM ACT 2006, 109 (2012).

47. CC v. Comm'r of Police of the Metropolis [2011] EWHC (Admin) 3316 (UK).

48. *Id.* at ¶¶ 11, 16, 18.

reasonable suspicion would, it is claimed, unduly compromise police capability to detect terrorism,[49] such as where a person is involved "unknowingly" or is of interest to the police based solely on their destination.[50] Reasonable suspicion requirements might also encourage the use of "clean skins," alert suspects to surveillance, and prevent the examination of—perhaps unwitting—travel companions.[51] To allay some of these concerns, an accompany Code of Practice issues an admonition not to discriminate or to select based on ethnic characteristics[52] and focuses selection based upon:

> Known and suspected sources of terrorism; Individuals or groups whose current or past involvement in acts or threats of terrorism is known or suspected, and supporters or sponsors of such activity who are known or suspected; Any information on the origins and/or location of terrorist groups; Possible current, emerging and future terrorist activity; The means of travel (and documentation) that a group or individuals involved in terrorist activity could use; Emerging local trends or patterns of travel through specific ports or in the wider vicinity that may be linked to terrorist activity. . .[; and/or] Observation of an individual's behaviour.[53]

In the case of *Miranda*, the initial view of the Security Service (MI5), which issued a "Port Circulation Sheet" to the police Counter Terrorism Command regarding Miranda, was that Schedule 7 was "Not Applicable."[54] These doubts were not conveyed to the examining officers on the ground. However, a third round of deliberations by the Security Service agents concluded that Miranda was concerned in terrorism because his mission sought to influence the government by promoting a political or ideological cause under the Terrorism Act 2000, section 1(1)(b) and (c).[55] In this way, the core argument in the case—internally in the security and policing agencies and later in court—was whether David Miranda could be categorised as a "terrorist" under section 40 of the Terrorism Act 2000:

> (1) In this Part "terrorist" means a person who—
> (a) has committed an offence under any of sections 11, 12, 15 to 18, 54 and 56 to 63, or
> (b) is or has been concerned in the commission, preparation or instigation of acts of terrorism.
> (2) The reference in subsection (1)(b) to a person who has been concerned in the commission, preparation or instigation of acts of terrorism includes a reference to a person who has been, whether

49. *Id.* at ¶ 9.

50. JOINT COMM. ON HUMAN RIGHTS, LEGISLATIVE SCRUTINY: ANTI-SOCIAL BEHAVIOUR, CRIME AND POLICING BILL (SECOND REPORT), 2013–14, H.L. 108, H.C. 951, ¶ 24 (UK).

51. ANDERSON, *supra* note 46, at 112.

52. HOME OFFICE, EXAMINING OFFICERS AND REVIEW OFFICERS UNDER SCHEDULE 7 TO THE TERRORISM ACT 2000: CODE OF PRACTICE, 2015, ¶ 4, at 6; ¶ 18, at 11 (UK).

53. *Id.* at ¶ 19, 11.

54. Miranda v. Sec'y of State of Home Dep't [2014] EWHC (Admin) 255 [9], [10] (UK).

55. *Id.* at [12].

> before or after the passing of this Act, concerned in the commission, preparation or instigation of acts of terrorism within the meaning given by section 1.[56]

In this case, section 40(1)(b) was claimed to be applicable, and so it required Miranda to be viewed in some way as being involved in "terrorism" as per the definition in the Terrorism Act 2000, section 1:

> (1) In this Act "terrorism" means the use or threat of action where—
>
> (a) the action falls within subsection (2),
>
> (b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and
>
> (c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.
>
> (2) Action falls within this subsection if it
>
> (a) involves serious violence against a person,
>
> (b) involves serious damage to property,
>
> (c) endangers a person's life, other than that of the person committing the action,
>
> (d) creates a serious risk to the health or safety of the public or a section of the public, or
>
> (e) is designed seriously to interfere with or seriously to disrupt an electronic system.[57]

Looking first at the issues of purpose and motive under section 1(1)(b) and (c), an alternative explanation to that latterly offered by the Security Service, which denies the applicability of section 1, might claim that the mission was one of revealing interesting facts in order to sell newspapers. This possibility was not proffered as such, and instead, Greenwald claimed before the High Court that the purpose of "responsible journalism" is the public interest,[58] an asserted privilege dismissed by the High Court on the basis that journalists have no such constitutional responsibility.[59] By comparison, a more convincing and limited claim to a purely journalistic mission was sustained in *R v. Murney*.[60] There, the collection of information about policing in Newry by an officer of *Eirígí*—a minor socialist Republican political party in Northern Ireland—was not an offence under the Terrorism Act 2000, section 58A—eliciting, publishing, or communicating information about members of the security forces which is of a kind likely to be useful for terrorism. While photographs of police activity could assist terrorism, the Crown Court in Belfast sustained that there was proof of a reasonable cause. The reasonable cause arose from genuine public concern about police abuses in circumstances where there was an ongoing protest in support of Republican Prisoners and the defendant was a participant in

56. Terrorism Act 2000, c. 11, §§ 40(1), 40(2) (UK).

57. *Id.* at §§ 1(1), 1(2).

58. *Miranda*, [2014] EWHC 255 at [55]. *See also* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

59. *Miranda*, [2014] EWHC 255 at [71].

60. R. v. Murney, [2014] NICC 4 (UK).

this protest as well as being the Public Relations Officer for *Eirígí*, which had organised the protest.

Returning to *Miranda*, as for the "action" element within section 1(1)(a) and section 1(2), section 1(2)(c) and (d) were the operative parts called in aid. The High Court decided that it was sufficient that the examining officers contemplated that the disclosure of data to a hostile state (Russia) or to terrorists, both of whom might be amongst the avid readership of publications based on the data, might imperil the identities of secret agents or the methods used for electronic surveillance of terrorists.[61] Thus, the material was placed in the realms of terrorism and not just official secrecy.[62] The formulation of "terrorism" in the mind of the examining officer did not require any specific offence to be formulated, nor must *mens rea*—beyond the "design" and "purpose" detectable from the mission—be established on the part of the traveller since there could be interest either in material being transported or in the traveller.[63] Nevertheless, the power must be exercised on "some reasoned basis, proportionately . . . and in good faith."[64] There was also no need to conclude that David Miranda was a person falling within section 40(1)(b) prior to the stop.[65] Nor did his express targeting exclude the exercise of Schedule 7 where the person had already fallen under suspicion; as stated in *CC v Commissioner of Police of the Metropolis*, "the language of s.40(1)(b) is wide enough to allow for examination not only of whether [a person] appears to be a terrorist but also of the way in which or the act by which he so appears."[66]

Having been satisfied that David Miranda could be categorised as a "terrorist" for the purposes of the Terrorism Act 2000, the final stage in the argument was to consider under administrative[67] and human rights law[68] whether the action taken was otherwise lawful. The High Court held that there was a compelling and proportionate interest to seize the data, especially as the Court denied the status of "journalistic materials" within Article 10, albeit on the dubious basis that they had been stolen.[69]

---

61. *Miranda* [2014] EWHC 255 at [24]–[25].

62. *Id.*

63. *Id.* at [34]; *see also* Zander, *supra* note 39.

64. *Miranda* [2014] EWHC 255 at [31].

65. *Id.* at [34].

66. CC v. Comm'r of Police of the Metropolis [2011] EWHC (Admin) 3316 [16] (UK).

67. For English administrative law, *see* Council of Civil Service Unions v. Minister for the Civil Service, [1985] AC 374 (appeal taken from Eng.); L. COMM'N, ADMINISTRATIVE LAW: JUDICIAL REVIEW AND STATUTORY APPEALS, Law Com. No. 226, HC 669 (H.M.S.O. 1994); L. COMM'N, ADMINISTRATIVE REDRESS: PUBLIC BODIES AND THE CITIZEN, Law Com. No. 322, HC 6 (H.M.S.O. 2012).

68. *See* Human Rights Act 1998, c. 42 (UK); *see generally* RICHARD CLAYTON & HUGH TOMLINSON, THE LAW OF HUMAN RIGHTS (2nd ed., 2009); TOM HICKMAN, PUBLIC LAW AFTER THE HUMAN RIGHTS ACT (2010); ALAN D.P. BRADY, PROPORTIONALITY AND DEFERENCE UNDER THE UK HUMAN RIGHTS ACT: AN INSTITUTIONALLY SENSITIVE APPROACH (2012).

69. Human Rights Act, c. 42, sch. 1, § 1 (3); *see also* Oxford v. Moss (1979) 68 Cr. App. Rep. 183 (Eng.) (ruling that information could not be deemed to be intangible

The Independent Reviewer of Terrorism Legislation[70]—David Anderson—commented that the High Court had endorsed so wide an ambit for the term "terrorism" that journalists and newspapers could potentially become subject to special criminal offences, could be proscribed—banned—, could be designated under terrorist asset-freezing legislation, and could be subjected to executive restraint orders.[71] At the same time, these potential calamities must be seen in the context of requirements of proportionality and respect for rights to free speech, so that *Miranda* made clear that "[t]here is no suggestion that media reporting on terrorism ought *per se* to be considered equivalent to assisting terrorists."[72]

As well as being stopped for "examination" under paragraph 2 of Schedule 7,[73] the traveller may also be searched under paragraph 8 by an examining officer or a person authorized under paragraph 10.[74] Property may be seized for investigation for seven days under paragraph 11. An increasingly common seizure scenario has involved the capture of data from laptops, data devices, and mobile phones. The practice has been to return the hardware within seven days but to retain the copied data in accordance with the guidance in the *Management of Police Information* ("MoPI"),[75] which suggests a six-year retention period.[76] Seizure of data, which was being transported for journalistic purposes, was at the heart of a further hearing in *R (Miranda) v Secretary of State for the Home Department and Commissioner of Police for the Metropolis*.[77] An interim hearing was held shortly after the examination in August 2013 concerning the seized computer data. It was held that inspection may take place for the purposes of securing national security or for the

property and therefore was incapable of being stolen within the Theft Act 1968); Grant v. Procurator Fiscal [1988] RPC 41 (Scot.).

70. *See* Terrorism Act 2006, c. 11, § 36 (UK).

71. DAVID ANDERSON, THE TERRORISM ACTS IN 2013: REPORT OF THE INDEPENDENT REVIEWER ON THE OPERATION OF THE TERRORISM ACT 2000 AND PART I OF THE TERRORISM ACT 2006, 28–32 (2014). The government's official response is to await the outcome of further litigation. *See* SECRETARY OF STATE FOR THE HOME DEPARTMENT, THE GOVERNMENT RESPONSE TO THE ANNUAL REPORT ON THE OPERATION OF THE TERRORISM ACTS IN 2013 BY THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, 2015, Cm. 9032 (UK).

72. Miranda v. Sec'y of State for the Home Dep't. [2014] EWHC 255, [35] (UK).

73. The term is mentioned but not defined by the Terrorism Act 2000, sch.7. It refers to the collection of powers affecting travellers under Schedule 7.

74. These provisions were reformed by the Anti-social Behaviour, Crime and Policing Act 2014, 2014, c. 12, sch. 9, following the OFFICE FOR SECURITY AND COUNTER-TERRORISM HOME OFFICE, REVIEW OF THE OPERATION OF SCHEDULE 7: A PUBLIC CONSULTATION (2012) (UK).

75. AUTHORISED PROFESSIONAL PRACTICE, *Information Management: Retention, Review, and Disposal*, COLLEGE OF POLICING (last updated July 28, 2015), https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/. This guidance is viewed as relevant by the HOME OFFICE, EXAMINING OFFICERS AND REVIEW OFFICERS UNDER SCHEDULE 7 TO THE TERRORISM ACT 2000: CODE OF PRACTICE (2015).

76. *See* R (RMC & FJ) v. Metro. Police Comm'r [2012] EWHC (Admin) 1681; M.M. v. United Kingdom (No. 157), 2012-IV Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/eng#{"appno":["\"24029/07\","],"documentcollectionid2":["GRANDCHAMBER", "CHAMBER"],"itemid":["001-114517"]}.

77. Miranda v. Sec'y of State for the Home Dep't. [2013] EWHC (Admin) 2609.

investigation of terrorism.[78] There was no exemption for journalistic materials.

Once the material is obtained under Schedule 7, it can be transferred to the security services under section 19(1) of the Counter Terrorism Act 2008, by which "[a] person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions." Furthermore, by section 19(6)(b), "[a] disclosure under this section does not breach . . . any other restriction on the disclosure of information (however imposed)." The data was transferred and retained even though Miranda was allowed to depart on his way after the detention under Schedule 7 had ended, and no further legal action had ensued either in relation to the data or Miranda—whose criminal *mens rea* might be compromised by the heavy encryption of the data. The High Court referred to the data being "stolen",[79] but Snowden had obtained copied data, and the hardware possessed by Miranda was not stolen property.[80] Consequently, no evident legal basis for police retention emerged to override paragraph 11.[81] Reflecting the need to keep up to date with technological developments,[82] as highlighted in the *Miranda* case, later legislation, the Anti-social Behaviour, Crime and Policing Act 2014, Schedule 9, paragraph 4 inserted paragraph 11A into Schedule 7. It grants an express power for police constables only[83] to make and retain copies of anything obtained from searches under paragraph 5, 8, or 9. Copies may be retained for as long as is necessary for investigative purposes or for use as evidence in criminal or deportation proceedings. However, retention is subject to the Data Protection Act 1998 and the MoPI guidance. Suggestions that these powers—and other search powers in Schedule 7—should be exercisable on reasonable suspicion[84] and that legally privileged and special procedure—including journalistic—material should be exempted were rejected during passage of the legislation through Parliament.[85]

Aside from the decision in *Miranda*, consideration was given in *Beghal v. DPP* to a wide catalogue of rights within the context of Schedule 7.[86] In 2011, Sylvie Beghal passed through East Midlands Airport

78. *Id.* at [32].

79. Miranda v. Sec'y of State for the Home Dep't. [2014] EWHC 255, [8] (UK).

80. *See* L COMM'N, *supra* note 67.

81. *See* Costello v. Chief Constable of Derbyshire [2001] EWCA (Civ) 381; Webb v. Chief Constable of Merseyside [1999] EWCA (Civ) 3041; Settelen v. Comm'r of Police of the Metro. [2004] EWHC 2171. One possible argument is that the Official Secrets Act 1989, 1989, c. 6, § 8, by which a Crown servant must take care to prevent the unauthorised disclosure of any document or article which it would be an offence under that legislation to disclose, makes it an offence to return data to Miranda because the return would involve a breach of offences in sections 1–4 of that Act by the police.

82. 9 July 2013, Parl Deb HC (6th ser.) (2013) col. 454 (UK).

83. *Id.* at col. 456.

84. 750 Parl Deb HL (5th ser.) (2013) col. 807 (UK); 751 Parl Deb HL (5th ser.) (2014) col. 497 (UK); JOINT COMMITTEE ON HUMAN RIGHTS, LEGISLATIVE SCRUTINY: ANTI-SOCIAL BEHAVIOUR, CRIME AND POLICING BILL, 2013–14, HL 56, HC 713, ¶ ¶112–13, 125 (UK).

85. 750 Parl Deb HL (5th ser.) (2013) col. 810 (UK).

86. Beghal v. DPP [2015] UKSC 49 (appeal taken from Gr. Brit.).

with her three children after visiting her husband, Djamel Beghal, in Paris, where he was detained on terrorist offences.[87] She was stopped by the police, which exercised its powers under Schedule 7 to question, search, and detain her for around 105 minutes. She was searched and was asked about her husband, her reasons for travel, and her travel arrangements. She refused to answer most of the questions and was charged under paragraph 18 with the offence of wilful failure to comply with the requirement to give the examining officer any information in her possession, which the officer requested. She later pleaded guilty to the offence and was sentenced to a conditional discharge. She then challenged whether her treatment had been consistent with her rights under the European Convention on Human Rights.[88]

The UK Supreme Court rejected the various human rights challenges in *Beghal*, reflecting the equal confidence on the part of the Home Office that the port controls are compliant with the European Convention on Human Rights following the reforms in the Anti-social Behaviour, Crime and Policing Act 2014,[89] having previously received assurances to that effect about anti-terrorism search powers in *Miranda*.[90]

As for the right to liberty under Article 5, a power to detain for at least this length of time was located within the exception for a stated legal "obligation" under Article 5(1)(b), with particular indulgence being shown for intrusions at borders and without the necessity for reasonable suspicion. This verdict was reached by the European Commission of Human Rights in regard to travellers to and from both parts of Ireland in *McVeigh, O'Neill, and Evans v. United Kingdom*[91] and in *Harkin, X, Lyttle, Gillen, and McCann v. United Kingdom*.[92] Next, in *Gillan and Quinton v. United Kingdom*, the European Court of Human Rights viewed the exercise of search powers at ports and airports as being excused by consent under Article 8.[93] Alternatively, the transitory

87. The Beghal family lived in France from 1990 to 1997 and then in the UK. On 15 March 2005, Djamel Beghal was convicted in France of "criminal association in relation with a terrorist undertaking" and sentenced to 10 years imprisonment. His French citizenship was stripped in July 2006, but attempts to deport him on the day of his release on 30 May 2009 to Algeria were stopped because of challenges on grounds of safety. He was released under house arrest conditions in France (the UK having formally excluded him in 2009) but was rearrested in 2011 and convicted in 2013 and sentenced to 10 years for involvement in the escape of Smain Ait Ali Belkacem, one of the attackers against the Metro station at the Museum Orsay in 1995.

88. *Supra* note 12.

89. *See* HOME OFFICE, MEMORANDUM ON THE EUROPEAN CONVENTION ON HUMAN RIGHTS, 2013, ¶ ¶ 192–93 (UK).

90. Miranda v. Sec'y of State for the Home Dep't. [2014] EWHC 255 [82], [88] (UK).

91. App. Nos. 8022, 8025, 8027/77 Eur. Comm'n H.R. Dec. & Rep. (1981); DR 18 p. 66 (admissibility), DR 25 p 15 (final report). *See also* R. Clayton and H. Tomlinson, The Law of Human Rights (2nd ed. 2009).

92. [1985] App. Nos. 11539, 11641, 11650, 11651, 11652/85 (UK), Ser A Vol.324 (1981).

93. Gillan and Quinton v. United Kingdom, App. No.4158/05, [64], 187 Eur. Ct. H.R. (2010). *See also* Gahramanov v. Azerbaijan, (2013) App. No.26291/06, (UK). A further challenge is pending in Malik v. United Kingdom, App. No.32968/11 (UK).

intrusion into a traveller's journey could even be viewed as not amounting to a deprivation of liberty at all.[94] As the wife of a convicted terrorist, the cause of her examination was evident under Article 5, while the examination power in general, though lacking any trigger of reasonable suspicion, was in fact applied in a discerning way to only 0.025% of travellers.[95]

Her Article 8 complaint was also not sustained because there are sufficient safeguards and controls against overbroad and arbitrary use, and the power is proportionately connected to the proper objective of Schedule 7, which is preventing and detecting terrorism and represents a level of intrusion which is comparatively light and not beyond the reasonable expectations of airport travellers in contemporary times of terrorist threat.[96] The UK Supreme Court also considered that there is also no substantial risk of these powers being used on a racially discriminatory basis, given the safeguards and the statistics, which show that the exercise of Schedule 7 powers is proportionate to the terrorist population.[97] The retention of electronic data could also be a justified intrusion into private life, though retention beyond the time of the examination should be based on objectively established grounds for suspicion.[98] This power was not applied to Beghal but was of course highly relevant to Miranda.

Finally, the UK Supreme Court also considered the issue of due process under Article 6, an aspect that conversely did not affect Miranda. The problem is that Schedule 7 affects the privilege against self-incrimination. It was accepted that the risk of criminal prosecution based on answers to Schedule 7 is negligible—though not impossible since the Director of Public Prosecutions refused to rule out a prosecution—since section 78 of the Police and Criminal Evidence Act 1984 would inevitably render such evidence inadmissible as unfair in any criminal trial.[99] Nevertheless, a port examination is not a form of crim-

94. *Id.* at 52–56. For the meaning of detention in this context, *see* R (Laporte) v. Chief Constable of Gloucestershire Constabulary [2006] UKHL 55; Austin v. Comm'r of Police of the Metropolis [2009] UKHL 5; Austin v. United Kingdom, App. Nos. 39692/09, 40713/09, 41008/09, Eur. Ct. H.R. (2012); Colon v. Netherlands, App. No. 49458/06, Eur. Ct. H.R. (2012); Roberts v. Comm'r of Police of the Metropolis [2015] UKSC 79.

95. *Id.* at ¶ 18. Lord Kerr (dissenting) viewed the potential for abuse as decisive. *Id.* at ¶ 102.

96. *Id.* at ¶¶ 43–51.

97. *Id.* at ¶ 50.

98. *Id.* at ¶¶ 57–58.

99. Police & Criminal Evidence Act 1984, c. 60, § 78 (Eng.):

> (1) In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

In Beghal's case, the denial of access to a lawyer may have rendered any admission to be unfair. *See* R (Elosta) v. Comm'r of Police for the Metropolis [2013] EWHC 3397 (Q.B.), ¶ 32 (Eng.); *see also* Anti-social Behaviour, Crime and Policing Act 2014, c. 12, ¶ 5, sch. 9 (Eng.) (Extending the rights in the Terrorism Act ("TA") 2000, Schedule 8, paragraphs 6 and 7, to have a named person informed of the fact of the detention and the right to consult a solicitor in private to persons detained at ports, airports, or interna-

inal investigation, so that Article 6 was deemed inapplicable.[100] Even in *Beghal*, it was silence that was incriminating rather than any answers she gave, and this distinction reflects a line of European Court of Human Rights decisions that have sometimes doubted the legitimacy of the use of forced answers in criminal proceedings rather than pressure to answer *per se*.[101] Once again, the attempt during the passage of the legislation to expressly exclude prosecution arising from forced answers was not successful.[102]

Whilst these findings of the U.K. Supreme Court equally rule out a range of challenges in circumstances such as in *Miranda*, they did not deal with any challenge based on freedom of expression under Article 10. Since none arose in *Beghal*, Article 10 was given no express recognition or protection in the Schedule 7 scheme when Article 10 was considered by the High Court in *Miranda*. That Court found no absolute rule of prior judicial scrutiny for cases involving State interference with journalistic freedom and relied on the doctrine of the margin of appreciation to uphold Article 10.[103] There was, however, some recognition of the tendency of the European Court of Human Rights to demand prior judicial authorisation for impingement upon confidential journalistic materials, though it was not viewed as an absolute rule.[104]

Perhaps with this warning in mind and perhaps in light of submissions from Parliament and from the Independent Reviewer of the Terrorism Legislation,[105] the Home Office significantly amended its Draft Code of Practice for examining officers and review officers under

---

tional rail stations. Furthermore, by paragraph 7A (paragraph 16A for Scotland), where a person detained for examination requests to consult a solicitor, questioning is suspended until the consultation has taken place or the person expresses a change of wishes. These rights may be qualified in the context of Schedule 7 detentions on extra grounds beyond those specified in the TA 2000, Schedule 8, where a person is not detained at a designated police station. The questioning may continue if the examining officer reasonably believes that postponement would prejudice the examination.).

100. *Id.* at ¶¶ 64–69. Lord Kerr (dissenting, ¶¶ 112–18) (calling in aid the wider concept of the privilege against self-incrimination at common law which requires only a "real and appreciable risk" of criminal proceedings being brought (citing *In re* Westinghouse Electric Corp. Uranium Contract Litig. MDL, Docket No. 235 (Nos. 1 and 2) [1978] AC 547 (HL) 574 (appeal taken from Eng.)) and applies to the risk of prosecution, not just conviction (citing Sociedade Nacional de Combustiveis de Angola UEE v. Lundqvist [1991] 2 Q.B. 310; JSC BTA Bank v. Ablyazov (No. 13) [2014] EWHC 2788)).

101. *See* Saunders v. United Kingdom, App. No. 19187/91, Eur. Ct. H.R (1996); IJL v. United Kingdom, App. Nos. 29522/95, 30056/96, 30574/96, Eur. Ct. H.R. (2000); O'Halloran & Francis v. United Kingdom, App. Nos. 15809/02, 25624/02, Eur. Ct. H.R. (2007). *See also* Procurator Fiscal v. Brown [2000] UKPC D3; Regina v. Allen [2001] UKHL 45.

102. *See* 750 Parl Deb HC (2013) col. 801 (UK); Sec'y of State for the Home Dept., The Gov't Response to the Annual Rep. on the Operation of the Terrorism Acts in 2012 by the Indep. Reviewer of Terrorism Legis., 2013, Parl. 1, at 9 (UK).

103. Roberts v. Comm'r of Police of the Metropolis [2015] UKSC 49 ¶ 88–89.

104. *Id.* at ¶ 88. *See* Sanoma Utigevers BV v. Netherlands, App. No. 38224/03 Eur. Ct. H.R. (2010); Telegraaf Media Nederland Landelijke Media BV v. Netherlands, App. No.39315/06 Eur. Ct. H.R. (2012); Nagla v. Latvia, App. No. 73469/10 Eur. Ct. H.R. (2013); Zakharov v. Russia, App. No. 47143/06 Eur. Ct. H.R. (2015).

105. Home Affairs Committee, Counter-Terrorism, 2013–14, H.C. 231, ¶ 93 (UK); Anderson, *supra* note 71, ¶¶ 7.31(b), Annex 2 ¶ 39.

Schedule 7 to the Terrorism Act 2000, which had been released in December 2014. Paragraph 40 originally stated that:

> The examining officer may copy any information obtained under paragraph 5; searched or found on a search under paragraph 8; or anything examined under paragraph 9 including electronic data (although examining officers should [cease reviewing, and] not copy information which they have reasonable grounds for believing is subject to legal privilege, as defined in section 10 of the Police and Criminal Evidence Act 1984).[106]

However, this paragraph was notably altered in the final version, which appeared in March 2015:

> The examining officer may copy any information obtained under paragraph 5; searched or found on a search under paragraph 8; or anything examined under paragraph 9 including electronic data (although examining officers should cease reviewing, and not copy, information which they have reasonable grounds for believing is subject to legal privilege, is excluded material or special procedure material, as defined in sections 10, 11 and 14 of the Police and Criminal Evidence Act 1984).[107]

Reference to "special procedure material" in section 14(1)(b) refers to "journalistic material, other than excluded material",[108] while "journalistic material" is defined in section 13 as follows:

> (1) Subject to subsection (2) below, in this Act "journalistic material" means material acquired or created for the purposes of journalism.
>
> (2) Material is only journalistic material for the purposes of this Act if it is in the possession of a person who acquired or created it for the purposes of journalism.
>
> (3) A person who receives material from someone who intends that the recipient shall use it for the purposes of journalism is to be taken to have acquired it for those purposes.[109]

Thus, if the facts of *Miranda* were to occur now, the officers should not deal with any such journalistic material under Schedule 7 and instead would have to invoke more formal powers to deal with "excluded materials", which are defined in section 11 to include journalistic materials held in confidence. The effect is that there would have to be resort to specific powers that allow for the search and retention of excluded materials, which would inevitably entail the important safeguard of an

106. HOME OFFICE, EXAMINING OFFICERS AND REVIEW OFFICERS UNDER SCHEDULE 7 TO THE TERRORISM ACT 2000: CODE OF PRACTICE ¶ 40 (July 2014). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/339197/schedule7.pdf.

107. HOME OFFICE, *supra* note 52, ¶ 40.

108. POLICE AND CRIMINAL EVIDENCE ACT 1984 § 14(1)(b), LEGISLATION.GOV.UK, http://www.legislation.gov.uk/ukpga/1984/60/contents.

109. *Id.* at § 13. *See* R v. Crown Court at Bristol, ex p Bristol Press and Picture Agency Ltd. (1986) 85 Cr. App. Rep. 190, DC (press photographs of riots were special procedure material).

application for a judicial warrant. One potential basis for such an application would be section 9 of the Official Secrets Act 1911:

> (1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorising any constable [named therein] to enter at any time any premises or place named in the warrant, if necessary, by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note, or document, or anything of a like nature or anything which is evidence of an offence under this Act having been or being about to be committed, which he may find on the premises or place or on any such person, and with regard to or in connexion with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.
>
> (2) Where it appears to a superintendent of police that the case is one of great emergency and that in the interest of the State immediate action is necessary, he may by a written order under his hand give to any constable the like authority as may be given by the warrant of a justice under this section.[110]

Alternatively, and even more likely, would be an application for a production order—or in default a search warrant—in relation to "excepted material"—which includes "excluded material"—under paragraph 5 of Schedule 5 of the Terrorism Act 2000.[111] The application can be made to a Circuit judge or a District Judge—Magistrates' Courts—for an order "for the purposes of a terrorist investigation."[112]

Schedule 7 returned to the U.K. courts with the Court of Appeal's decision in *Miranda* in January 2016.[113] The judgment included some radical departures from the High Court verdict, but without fundamentally altering the outcome. The same depiction of Miranda was accepted, as before—he was primarily a terrorist threat and not a national security threat, which meant that the invocation of Schedule 7 was lawful.[114] It was further held that the police were entitled to consider whether material in the possession of Miranda might be released in circumstances falling within the definition of "terrorism" and therefore had sufficient "grounds" to detain him in relation to which:

> Parliament has set the bar for the exercise of the Schedule 7 power at quite a low level . . . . [T]he power has been given to provide an opportunity for the ascertainment of the *possibility* that a traveller at a port may be concerned in the commission, preparation or instigation of an act of terrorism.[115]

110. Official Secrets Act 1911, 1 & 2 Geo. 5 c. 28, § 9 (UK).

111. *See* CLIVE WALKER, TERRORISM AND THE LAW, 57–58, §2.16 (Carlile of Berriew et. al. eds., 2011).

112. *Id.* at 60.

113. Miranda v. Sec'y of State for the Home Dep't [2016] EWCA Civ 6 (UK).

114. *Id.* at ¶ 34.

115. *Id.* at ¶¶ 57–58.

Nor was it necessarily unjustified or disproportionate to take action just because Miranda was involved in journalism.[116]

In two important respects the Court of Appeal departed from the reasoning of the High Court. First, the definition of "terrorism" was revised. The Court of Appeal held that a mental element must, contrary to what it accepted as the literal interpretation, be met in relation to the element of action within section 1(2), meaning that intent or recklessness as to the action within section 1(2) of the Terrorism Act 2000 must be proven.[117] A number of reasons were adduced for this abrupt discovery, overlooked by previous courts, such as the UK Supreme Court in *R v. Gul*, which stated that "[d]espite the undesirable consequences of the combination of the very wide definition of 'terrorism' and the provisions of section 117, it is difficult to see how the natural, very wide, meaning of the definition can properly be cut down by this Court."[118] None of the reasons given by the Court of Appeal for the radical departure are wholly convincing.

First, the Court of Appeal had to accept that its reasoning was uneven and incomplete. For these purposes, the Court of Appeal divided "action" in section 1(2) into three categories.[119] The first was section 1(2)(a) and (b), which, since it describes a person as being "involved" in violence or damage to property must require awareness that he is being so involved, though "involved" could equally refer to causation as to intent. The third category was section 1(2)(e) which is defined according to its aim and, therefore, was said to be clearly defined by reference to the state of mind of the actor, though "aim" could be satisfied by motive and purpose as well as intent. More difficult for the Court of Appeal was its second category, section 1(2)(c) and (d), which relates to the consequences of actions and which could, on a literal interpretation, include acts which endanger life by design even if the actor is not subjectively aware that they do. At best, the Court of Appeal had to overcome this variation on the basis that:

> [i]f Parliament had intended to provide that a person commits an act of terrorism where he unwittingly or accidentally does something which in fact endangers another person's life, I would have expected that, in view of the serious consequences of classifying a person as a terrorist, it would have spelt this out clearly.[120]

A closely related argument was that the Court of Appeal viewed the absence of *mens rea* as creating overreach: "[terrorism] would include activity that is entirely non-violent; is in pursuit of a legitimate and mainstream political cause; may 'endanger life' by accident; and where the person may be 'concerned' in such activity wholly accidentally or even without knowledge."[121] Examples were adduced of unpalatable

116. *Id.* at ¶ 82.
117. *Id.* at ¶ 55.
118. R v. Gul [2013] UKSC 64, ¶ 38 (appeal taken from Eng.).
119. Miranda v. Sec'y of State for the Home Dep't [2016] EWCA Civ 6 at ¶¶ 53–54 (UK).
120. *Id.* at ¶ 54.
121. *Id.* ¶ 43.

instances of "terrorism", including agitation—on religious or political grounds—against the vaccination of children for certain diseases; or circumstances where a group of protesters erect a sign to protest about Government policy which is inadvertently erected in a way that accidentally endangers the life of a passer-by.[122] Yet, these effects and overbreadth can conceivably be resolved without the insertion of mens rea. In particular, the elements of motive and purpose in section 1 could hardly be satisfied by accident. If the actions were not being carried out with a specified purpose or with the requisite motive, then section 1 is not satisfied. Some level of self-awareness is required, but this is not the same as mens rea. Furthermore, overbreadth is expressly confronted in other ways by the legislative scheme, including by a special independent review mechanism under the Terrorism Act 2006, section 36, and by the requirement for consent to prosecution by the Director of Public Prosecutions or, in some cases, by the Attorney General under section 117 of the Terrorism Act 2000.[123]

The second reason of the Court of Appeal was based on legislative history. It mentioned that when introducing the Terrorism Act 2000, the Home Secretary, Jack Straw, argued in Parliament that "[terrorism] is premeditated, and aims to create a climate of extreme fear."[124] Unfortunately, the Court of Appeal also failed to note that Straw went on to say, "[c]lause 1 does not create an offence of terrorism. It sets out the extremely specific circumstances in which the use of police powers can be triggered or in which the use of other powers can be triggered—also in very controlled circumstances."[125] In the circumstances, "premeditated" could again refer as much to motive and purpose as to any element of intent.

Though not so clearly engaged with by the Court of Appeal, a third reason to doubt its conclusion, hinted at by Jack Straw, is legislative purpose. The fundamental idea of the legal concept of terrorism is to move on from the confines of the jurisprudence of crime. Section 1 does not create any criminal offence,[126] nor does it derive from criminal law concepts.[127] Instead the term is mainly conceived and used as a basis for pre-emptive action by the police and executive—such as in the proscription of organisations, financial controls and other personal restrictions on suspects, and wide investigative powers for the police. True enough, the term "terrorism" is embodied in various special crimi-

122. *Id.* ¶¶ 45–46. These examples derive from D. Anderson, THE TERRORISM ACTS IN 2014: REPORT OF THE INDEPENDENT REVIEWER ON THE OPERATION IN 2014 OF THE TERRORISM ACT 2000 AND PART I OF THE TERRORISM ACT 2006 (2015) ¶¶ 4.14–4.21.

123. As mentioned by the U.K. Supreme Court in R v. Gul [2013] UKSC 64, ¶¶ 30, 34.

124. HC Deb 14 December 1999 vol 341 col 152.

125. *Id.* at col.156. *Cf.* [2016] EWCA Civ 6 at ¶ 49, which not only takes the first quote out of context but also gives a faulty reference.

126. *See* Miranda v. Sec'y of State for the Home Dep't. [2014] EWHC 255, ¶ 29 per Laws LJ. Proposals to enact a crime of terrorism have long been rejected in the U.K. Clive Walker, TERRORISM AND THE LAW, ch. 5 (Oxford University Press, Oxford, 2011).

127. For the history, *see* C. Walker, TERRORISM AND THE LAW, ch. 1 (Oxford University Press, Oxford, 2011).

nal offences, especially in Part VI of the Terrorism Act 2000. But elements of *mens rea* can be added at that point alone, and there is also the filter of consent to prosecution as already mentioned. This point about distinct legislative purpose is also underlined by considering the formulation in section 1—and in its predecessor, section 20(1) of the Prevention of Terrorism (Temporary Provisions) Act 1989[128]—as distinct from the reliance upon a list of offences—"scheduled offences" in the Northern Ireland (Emergency Provisions) Acts 1973–98. In this way, section 1 keeps away from any direct link between criminal law and the phenomenon of terrorism.

The second major departure by the Court of Appeal from the decision of the High Court was its conclusion that the way in which Schedule 7 could be conducted against journalists was not adequately "prescribed by law" to be within any exception to Article 10 of the European Convention on Human Rights: "TACT, therefore, contains no adequate legal safeguards relating to journalistic material *simpliciter* or to journalistic material the disclosure of which may identify a confidential source. Nor are any such safeguards to be found in any other rules operating within the framework of law."[129] In this way, the requirements in cases such as *Sanoma Utigevers BV v Netherlands*,[130] in which the Grand Chamber held that a Dutch law authorizing the compulsory surrender of material to the police for use in a criminal investigation was repugnant to Article 10, were viewed as more "absolute" than had been depicted in the High Court. The requirements included the following: first, "the protection of journalistic sources . . . must be attended with legal procedural safeguards commensurate with the importance of the [Article 10] principle at stake . . . ."[131] Second, "[f]irst and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body [of any requirement that a journalist hand over material concerning a confidential source] . . . ."[132] Third, "the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure . . . ." The decision to be taken should be governed by clear criteria . . . ."[133] Fourth, "the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality"[134] and cannot therefore constitute a legal procedural safeguard commensurate with the rights protected by Article 10. Fifth, however, where "it may be impracticable for the prosecuting authorities to state elaborate reasons

128. "'[T]errorism' means the use of violence for political ends and includes any use of violence for the purpose of putting the public or any section of the public in fear." Prevention of Terrorism (Temporary Provisions) Act 1989 c. 4 §20 (1).

129. Miranda v. Secretary of State for the Home Department [2014] EWCA Civ 6, ¶ 115.

130. Sanoma Uitgevers B.V. v. Netherlands, Eur. Ct. H.R. (2010).

131. *Id.* at ¶ 88.

132. *Id.* at ¶ 90.

133. *Id.* at ¶ 92.

134. *Id.* at ¶ 91.

for urgent orders or requests . . . an independent review carried out at the very least prior to the access and use of obtained materials should be sufficient to determine whether any issue of confidentiality arises, and if so, whether . . . the public interest invoked by the investigating or prosecuting authorities outweighs the general public interest of source protection."[135]

The emphasis placed on the judiciary is somewhat at odds with the Court of Appeal's view that "[t]he police and the Security Service have the expertise and access to secret intelligence material which rightly make it very difficult to challenge such an assessment in a court of law."[136] Nevertheless, since Schedule 7 failed to incorporate safeguards for journalistic materials, which either did disclose sources or might reveal sources, the provision was held to be incompatible with Article 10.[137] This declaration, made under section 4 of the Human Rights Act 1998, does not invalidate Schedule 7—or the finding in the case that the action was lawful on the facts as applied—but it does send a strong signal to the executive and Parliament that reform is needed. The Court of Appeal did not explicitly consider whether the subsequent changes made in 2015 to the Code of Practice, discussed above, would meet their concerns. However, the Home Office made such an argument in the wake of the judgment.[138] The Code of Practice could be a sufficient instrument to be 'in accordance with the law' under Article 10, though a more explicit piece of legislation may be advisable for such an important issue as journalistic freedoms.[139]

Assessing the impact of Schedule 7 port controls on journalism in light of *Miranda*, it must be concluded that the special laws became rather strained—especially through the discovery of the *mens rea* requirement—and were fundamentally ill-designed to handle the important media rights at stake. An even broader power to examine and search for materials, the possession of which is contrary to U.K. law, has been suggested as a more suitable legal vehicle than Schedule 7 or rules as to imports and exports—such as weapons—or customs dues.[140] Materials held in breach of official secrets laws could thereby be expressly sought. However, a less ambitious reform emerged in 2015, namely, to insert within the port controls recognition of journalistic

135. *Id.* at ¶ 91.

136. *Id.* at ¶ 82.

137. *Id.* at ¶ 114.

138. *Airport stop of Snowden reporter's partner David Miranda 'lawful'*, BBC NEWS, http://www.bbc.co.uk/news/uk-35343852, (last visited Jan. 19, 2016).

139. A similar model is contained in Part II of the Criminal Justice and Police Act 2001, where the police can bundle up and take away for further sifting materials found in a physical search; once they come across special procedure material, they have to apply to a judge. Criminal Justice and Police Act, 2001 s.55 (UK).

140. There exists a broad power to 'rummage' in the prevention of smuggling under the Customs and Excise Management Act 1979, s.27 (UK). For import and export controls, see Import of Goods (Control) Order 1954, SI 1954/23 (UK); Import and Export Control Act 1990 (UK); Export Control Act 2002 (UK); Export Control Order 2008, SI 2008/3231 (UK); Zeray Yihdego & Ashley Savage, *The UK Arms Export Regime: Progress and Challenges*, 2008 PUBLIC LAW 546 (2008).

interests, though whether a Code of Practice represents a sufficient degree of recognition remains to be determined. Arguably with that reform in place, the more significant outcome could be the refinement of the definition of terrorism. However, as the new interpretation did not avail David Miranda and might also be viewed by the Home Office as warding off any troublesome rewriting of section 1, an uneasy but convenient settlement may have emerged for now, which will unfortunately avert any impetus to reform the definition of terrorism.

III. Demand for Information

Cooperation between police and media is ingrained in both low and high policing.[141] There are two common modes of engagement. The principal mode of relationship is managerial.[142] In this mode, the police, albeit that they are powerful initiators in criminal justice and can wield coercive powers, are concerned with news management—how information is released and understood through negotiation and interaction. Underlying this approach is a high degree of cooperation and mutual reliance between police and media, as well as recognition by the police of the independence and important roles of the media. Consequently, many previous researchers have found that there is often a stable and productive relationship between the police and crime reporters.[143] Thus, there is "a sense of dependency between police and members of the media, uneasy though this may be at times."[144] While the police may sometimes seek to manipulate media coverage of their image and work,[145] they also depend on the media for the regular conveyance of messages to the public and at times utilize the media as an investigative resource.[146] In turn, journalists depend upon the police for primary information. It is difficult to be conclusive about which side acts as primary information-gatekeeper. Without hard law to regulate self-serving relationships, temptations to give and take may arise and have indeed been at the heart of inquiries into press conduct in relation to telephone tapping and other breaches of privacy in the United

141. *See generally* Jean-Paul Brodeur, *High Policing and Low Policing: Remarks About the Policing of Political Activities*, 30 Soc. Probs. 507 (1983). *See also* Clive Walker, *The Police and the Mass Media in Emergencies*, 1 Hum. Rts. Rev. 15 (2011).

142. Walker, *supra* note 141 at 15.

143. *See, e.g.*, Philip Schlesinger & Howard Tumber, Reporting Crime: the Media Politics of Criminal Justice (Oxford Univ. Press ed., 1994); Richard V. Ericson, Crime and the Media (Open Univ. Press 1995); Crime and the Media: The Post Modern Spectacle (David Kidd-Hewitt & Richard Osborne eds., 1995); Dennis Howitt, Crime, the Media and the Law (Wiley ed., 1998); Steve Chibnall, Law and Order News: An Analysis of Crime Reporting in the British Press (Routledge ed., 2001); Maggie Wykes, News, Crime and Culture (Pluto Press ed., 2001); Rob C. Mawby, Policing Images: Policing Communication and Legitimacy (Willan ed., 2002); Frank Leishman & Paul Mason, Policing and the Media: Facts, Fictions and Factions (Willan ed., 2003).

144. Frank Leishman & Paul Mason, Policing and the Media: Facts, Fictions and Factions 31 (Willan ed., 2003).

145. *See* Home Affairs Committee, Police and the Media, 2008–09, HC 75, ¶ 29 (UK).

146. *See* Martin Innes, *The Media as an Investigative Resource in Murder Enquiries*, 39 Brit. J. Criminology 269 (1999).

Kingdom in recent years.[147] One major impact was the closure of the *News of the World* newspaper in 2011. Journalists have also been convicted of breaches of the Data Protection Act of 1998 and the Regulation of Investigatory Powers Act of 2000,[148] while police and other collaborators within officialdom have also been convicted of corruption.[149]

The second mode for police-media relations is coercive.[150] In certain circumstances, the police can coerce the media into action or inaction through the application of legal powers. One such application might involve the use of the media as surrogate investigators and information sources. This mode of relationship is not common in the United Kingdom. Freedom of the press is highly valued in United Kingdom constitutional law, as evidenced by the special protection for "freedom of expression" in section 12 of the Human Rights Act of 1998, which builds upon the European Convention on Human Rights and Fundamental Freedoms of 1950, Article 10.[151] Nevertheless, the coercive demand for information may arise under threat of legal powers or under the actual invocation of legal powers. In either case, there is a strong element of coercion and threat.

This modality arose in the *Miranda* case. On 20 July 2013, even before the Heathrow Airport incident—which occurred on 18 August 2013—but revealed after that event, *The Guardian* disclosed that GCHQ had forced the newspaper to destroy Snowden-related documents or face legal action. The authorities told the paper, "[y]ou've had your fun. Now we want the stuff back."[152] The materials were held in the basement of the newspaper's offices. In the presence of GCHQ technicians, a senior editor and a *Guardian* computer expert used angle grind-

147. *See* INFORMATION COMMISSIONERS OFFICE, WHAT PRICE PRIVACY? THE UNLAWFUL TRADE IN CONFIDENTIAL PERSONAL INFORMATION, 2006, HC 1056 (UK); *see also* INFORMATION COMMISSIONERS OFFICE, WHAT PRICE PRIVACY NOW? THE FIRST SIX MONTHS PROGRESS IN HALTING THE UNLAWFUL TRADE IN CONFIDENTIAL PERSONAL INFORMATION, 2006, HC 36 (UK); THE LEVESON INQUIRY, AN INQUIRY INTO THE CULTURE, PRACTICES AND ETHICS OF THE PRESS: EXECUTIVE SUMMARY, 2012–13, HC 779 (UK); CULTURE, MEDIA AND SPORT COMMITTEE, NEWS INTERNATIONAL AND PHONE-HACKING, 2010–12, HC 903-I (UK); HOME AFFAIRS COMMITTEE, UNAUTHORISED TAPPING INTO OR HACKING OF MOBILE COMMUNICATIONS, 2010–12, HC 907 (UK); SECRETARY OF STATE FOR THE HOME DEPARTMENT, THE GOVERNMENT RESPONSE TO THE THIRTEENTH REPORT FROM THE HOME AFFAIRS COMMITTEE SESSION, 2010–12, HC 907 (UK): UNAUTHORISED TAPPING INTO OR HACKING OF MOBILE COMMUNICATIONS, Cm. 8182 (UK); COMMITTEE OF PRIVILEGES, FIRST SPECIAL REPORT: MATTER OF PRIVILEGE REFERRED TO THE COMMITTEE ON 22 MAY 2012, 2014 HC 903-I (UK).

148. Coulson & Kuttner v. Regina [2013] EWCA (Crim) 1026, (appeal taken from Eng.). (Case includes Clive Goodman (2007); and Dan Evans, Graham Johnson, Ian Edmondson, Neville Thurlbeck, Greg Miskiw, James Weatherup, Andy Coulson (R v. Coulson & Kuttner [2013] EWCA (Crim) 1026); and Anthony France (2015).

149. *See generally* Alan King & Paul Marshall (2005); Alan Tierney & Richard Trunkfield (2013); Paul Flattley (2013); James Bowes (2013); April Casburn (2013); Timothy Edwards (2014).

150. Miranda v. Secretary of State for the Home Department [2014] EWCA Civ 6.

151. Human Rights Act, *supra* note 68.

152. Alan Rusbridger, *David Miranda, schedule 7 and the danger that all reporters now face*, THE GUARDIAN (Aug. 20, 2013), http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters.

ers and drills to "pulverise the hard drives and memory chips on which the encrypted files had been stored."[153] It was appreciated that the destruction was a show of force, because all parties knew that other copies of the data were held elsewhere—in Russia, the U.S., Brazil, and China. But the authorities wanted this destruction to take place to at least ensure the security of sensitive data within the United Kingdom. The newspaper complied, fearing either a civil injunction or criminal proceedings under the Official Secrets Act of 1989. In any event, they chose to destroy the documents rather than hand them over so as to avoid any extraneous markings and also to avoid revealing the extent of their catalogue.

If the obliteration of journalistic materials under threat of legal action does not sound drastic enough, more legalistic coercion can actually be invoked. Again, this approach is not novel, and legal activities in connection with infractions of the Official Secrets Acts 1911–89 have already been noted. But demands for information are becoming firmly attached to counterterrorism operations, as revealed in two ways.

The first aspect concerns the use of special search powers in Schedule 5 of the Terrorism Act of 2000—already mentioned as a possible power, which might have been invoked in the *Miranda* case.[154] Schedule 5 offers variants upon production and search powers in relation to potential evidence contained in Schedule 1 of the mainstream policing legislation—namely, the Police and Criminal Evidence Act of 1984 ("PACE"). The main differences between the Terrorism Act powers and the PACE powers are the triggering criteria, which relate to "terrorist investigations" rather than to specified criminal offences, and the more extensive powers so triggered. The catalogue includes powers to enter premises, to search the premises or any person found there, and to seize and retain any relevant material. By Schedule 5, paragraph 1(1): "[a] constable may apply to a justice of the peace for the issue of a warrant under this paragraph for the purposes of a terrorist investigation." The premises to be targeted may be particular—for a "specific premises warrant"—or, following amendment by the Terrorism Act of 2006, section 26, they may comprise any or sets of premises occupied or controlled by a person specified in the application—an "all premises warrant."[155] "Excepted material" may not be the subject of an application, and that term is defined in paragraph 4 by reference to corresponding PACE exceptions. These comprise "excluded material" (under section 11 of PACE, which includes journalistic material which a person holds in confidence and which consists of documents or of records other than documents), "special procedure material" (under section 14 of PACE, which includes all other journalistic material, other than excluded material), and "items subject to legal privilege" (under

153. Julian Borger, *NSA files: why the Guardian in London destroyed hard drives of leaked files*, THE GUARDIAN (Aug. 20, 2013), http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.

154. *See* Terrorism Act 2000, c. 11, sch. 5 (UK).

155. *Id.*; *see* Redknapp v. City of London Police [2008] EWHC (Admin) 1177 (indicating that a warrant may incorporate both formats).

section 10 of PACE). Journalistic material is defined in section 13 of PACE, as already described.[156]

In the light of these exceptions, the Terrorism Act of 2000's search powers have not been recorded as being used against journalists, but an attempt to secure information from *The Guardian* and *The Observer* about possible breaches of official secrets legislation was made in *R v. Central Criminal Court, ex parte Bright.*[157] A decade and a half ago, the judgment emphasized the value of journalism:

> [P]remises are not to be entered by the forces of authority or the State to deter or diminish, inhibit or stifle the exercise of an individual's right to free speech or the press of its freedom to investigate and inform . . . . Inconvenient or embarrassing revelations, whether for the Security Services, or for public authorities, should not be suppressed.[158]

More threatening is the next investigative power, under Schedule 5, paragraph 5, which deals with the production of, or access to—rather than the physical search for—"excluded" and "special procedure" materials.[159] By paragraph 8, only legally privileged material is wholly exempted from the clutches of paragraph 5. By paragraph 5(1), a constable may apply to a circuit judge for a production order to access excluded or special procedure material—including, under paragraph 7, material coming into existence within 28 days—for the purposes of a terrorist investigation.[160] There is no requirement that notice be given to the possessor of the materials or that the material must be potential "evidence" for a court case. If granted, the order may require under paragraph 5(3), normally within seven days, a specified person: (a) to produce to a constable within a specified period for seizure and retention any relevant material; (b) to give a constable access to relevant material within a specified period; and (c) to state to the best of his knowledge and belief the location of relevant material if it is not in, and will not come into, his possession, custody, or power within the period specified under (a) or (b). An order may also require any other person who appears to the judge to be entitled to grant entry to the premises to allow entry and access.[161] The circuit judge may grant an order if the request "satisfies" two conditions in paragraph 6. The first condition relates to the relevance to the purposes of a terrorist investigation, as well as the need for "reasonable grounds for believing that the material is likely to be of substantial value." The second condition demands reasonable grounds for believing that it is in the public interest that the material should be produced. Under paragraph 10, the order is treated

156. Police and Criminal Evidence Act 1984, c. 60 (UK).

157. R v. Central Criminal Court, *ex parte* Bright [2000] EWHC 560.

158. *Id.* ¶¶ 97–98.

159. Terrorism Act 2000, *supra* note 154.

160. *Id.* at 5(1).

161. *Id.* at 5(3).

as if it were an order of the Crown Court and can be enforced by contempt of court powers.[162]

Much of the litigation arising from Schedule 5, paragraph 5 has related to journalistic materials.[163] In *R v. Middlesex Guildhall Crown Court, ex parte Salinger & Anor*,[164] the police sought to obtain from the prominent U.S. journalist, Pierre Salinger, and his media employers, records of interviews conducted in Libya with the two prime suspects of the Lockerbie bombing in 1988. On the initial *ex parte* application, the High Court held that the police should provide to the judge a written statement of the material evidence, including the nature of the available information subject to secrecy and sensitivity, and the applicant police officer should appear before the judge to provide oral evidence. The judge could then decide on the grant of the order and also on what information might be served on the recipients. In turn, the recipients will rarely be notified until the service of the order,[165] when they are entitled to be given, preferably in writing, as much information as could properly be provided as to the grounds for the order; however, it is rarely appropriate or necessary for disclosure of the source or details. Their subsequent application to discharge or vary should be made to the same judge with the same police officer who gave oral evidence being present. On this application, the judge can reconsider the order afresh on its merits, and there is no onus on the recipient to satisfy the judge that the order was wrongly made. It was later revealed that ABC News had agreed to comply because the order did not require the disclosure of confidential sources.[166]

Journalistic material was again investigated in 1991 when Box Productions compiled a television programme, broadcast by Channel 4. It alleged collusion between members of the Royal Ulster Constabulary and Loyalist terrorists, which was presided over by a secret committee of prominent people in Northern Ireland. The police sought the production of documents connected with the programme. A redacted dossier of material was handed over, but it was claimed that further sensitive material had either been destroyed or removed from the jurisdiction and that the only person who knew the whereabouts of the material was a researcher employed by Box Productions. The judge then directed that the material sent abroad should be brought back and produced to the police. The respondents refused to comply. The Divisional Court, which could not review the judge's order, imposed a fine of £75,000 for contempt.[167]

---

162. *Id.* at 6 (2); *see also* Criminal Procedure Rules 2013, SI 2013/1554, §§ 6.6, 6.7, 6.13. *Ex parte* hearings may arise under §§ 6.3(3), 6.12.

163. *See also* In re Request from the United Kingdom, 718 F.3d 13 (1st Cir. 2013).

164. R v. Middlesex Guildhall Crown Court, *ex parte* Salinger & Anor [1993] QB 564.

165. *See also* Re Morris [2003] NICC 11. But appearance might be allowed in difficult and complex cases involving the media. *Id.* at ¶ 35.

166. *See* W.E. Schmidt, *British TV Station Defies Order to Identify Source,* N.Y. TIMES, May 3,1992, at 10.

167. *See generally* DPP v. Channel 4 & Box Productions [1993] 2 All ER 517. *See also* R. Costigan, *Further Dispatches*, 142 NEW L. J. 1417 (1992); S. MCPHILEMEY, THE COMMITTEE

Next, in *Re Moloney's Application*,[168] the Northern Ireland editor of the *Sunday Tribune* newspaper was required to produce notes of an interview with William Stobie, who was later accused of the murder of a prominent lawyer, Patrick Finucane.[169] Quashing the Recorder's order, the High Court stated, "[t]he police have in our view to show something more than a possibility that the material will be of some use. They must establish that there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation."[170]

In *Re Jordan*,[171] the police sought materials from a BBC *Panorama* programme, *Gangsters at War*, which transmitted an announcement by a masked man on behalf of the Ulster Freedom Fighters. He was identified through voice analysis as Dennis Cunningham.[172] Any arguments about the chilling effect of disclosure on the ability to carry out investigative journalism were outweighed in the view of the Crown Court in Belfast by "the unmasking of terrorists and bringing them to justice."[173]

By contrast, the BBC escaped compulsory disclosure by the Belfast Recorder's Court of un-broadcast film of a Republican parade in Londonderry in 2011 in which a masked man read out a speech on behalf of the Real IRA.[174] The police's claim that the extra footage would aid identification was rejected under Schedule 5, paragraph 5, because no "substantial value" had been established by the police. However, the court made clear that if the police had met the standard of proof, the public interest would have outweighed claims by the media of increased risks in news-gathering.

In *Malik v. Manchester Crown Court*,[175] a production order was granted in relation to a book manuscript written about Hassan Butt, entitled *Leaving Al-Qaeda*. The police believed that the materials possessed by Malik, who helped to write the book, might disclose evidence of crimes by Butt. It was held that "likely," paragraph 6(2)(b) demanded a high standard—"probable"—but "substantial value" required only a value more than minimal.[176] Being "satisfied" required a firm belief rather than a suspicion.[177] On review, the grant of the order was upheld, though the terms were altered. The High Court indicated that a court could, of its own motion, appoint a special advocate

(Robert Rinehart ed., 1999); McPhilemy v. Times Newspapers Ltd. [2001] EWCA (Civ) 933 (Eng.).

168. Re Moloney's Application [2000] NIJB (Civ) 195, (N. Ir.).

169. *See* Sir D. de Silva, REPORT OF THE PATRICK FINUCANE REVIEW, 2012, HC 802 (UK).

170. Re Moloney's Application [2000] NIJB at 207.

171. Re Jordan [2003] NICC 17 (N. Ir.).

172. *See* R v. Cunningham [2005] NICC 45 (N. Ir.) (regarding the conviction of Dennis Cunningham).

173. Re Jordan [2003] NICC 17, ¶ 1 (N. Ir.).

174. *See* BBC v. PSNI [2012] NICty 1 (N. Ir.).

175. Malik v. Manchester Crown Court [2008] EWHC (Admin) 1362.

176. *See id.* at ¶ 36.

177. *See id.* at ¶ 37.

to appear at the *ex parte* hearing or on an application for variation or discharge, but only in exceptional cases.[178]

In *Re Galloway*, the Police Service of Northern Ireland sought records and materials from the Northern Editor of the *Sunday Tribune* newspaper relating to claims of responsibility for the murders by Republican dissidents of two soldiers in 2009.[179] The application was refused. The Court endorsed the approach that the public interest in the investigation and prosecution of serious crime is important, so the level of proof of overriding interests must attain a very high threshold of a substantial risk—in this case, the threat to the right to life (Article 2 of the Convention) of the journalist and her family. In that case, the journalist met the standard.[180]

Two issues have not yet been adequately litigated. The first involves whether compliance with the production order might involve forcible self-incrimination contrary to Article 6 of the European Convention on Human Rights. It was indicated in *R v. Central Criminal Court, ex parte Bright* that the statutory powers of production override any right against self-incrimination.[181] Equally, claims under Article 6 were dismissed in *Beghal*, as already indicated.[182] The production of physical materials with an existence independent of the will of the defendant has been treated in the jurisprudence of the European Convention on Human Rights as distinct from demanding information from the knowledge of the defendant.[183]

The second factor to be further explored is the impact of section 12(4) of the Human Rights Act of 1998, which requires "particular regard" for the importance of freedom of expression before any order is granted. Section 12 was enacted to "tip the balance" in favour of expression.[184] Its weighting has not yet made any impact in any of the cases cited above.

Should a production order under paragraph 5 of the Terrorism Act 2000 be viewed as inappropriate for the purposes of the investigation, a constable may apply to a circuit judge—or in Northern Ireland, a Crown Court judge—under paragraph 11 for the issuance of a warrant to permit entry, search, and seizure.[185] This variant procedure may be selected where, under paragraph 12, a circuit judge is satisfied that a production order has not been complied with, or where he is satisfied that there are reasonable grounds for believing there is material likely to be of substantial value, but that it is not appropriate to

178. *See id.* at ¶ 99.

179. *See generally* Re Galloway [2009] NICty 8 (N. Ir.).

180. *Id.* at ¶ 8.

181. R v. Central Criminal Court, *ex parte* Bright, [2000] EWHC (QB) 662 (Eng.).

182. Beghal v. DPP [2015] UKSC 49 (appeal taken from Gr. Brit.).

183. *See* O'Halloran v. United Kingdom, 46 Eur. Ct. H.R. 21 (2008).

184. Human Rights Act, *supra* note 68. *See* CLAYTON & TOMLINSON, *supra* note 68, at ¶ 15.22. *See also* Stephen Tierney, *Press Freedom and Public Interest: The Developing Jurisprudence of the European Court of Human Rights*, 4 EUR. HUM. RTS. L. REV. 419 (1998).

185. Terrorism Act 2000, *supra* note 154, at 12.

proceed by way of production order—perhaps because it would tip off a potential collaborator.[186]

Another type of investigative power is ancillary to the foregoing. Pursuant to Schedule 5, paragraph 13, a constable may apply to a circuit judge—or in Northern Ireland, a Crown Court judge—for an order requiring any person specified in the order to provide an explanation of any material seized, produced, or made available under paragraphs 1, 5, or 11.[187] There is no immunity against revealing information concerning other excepted materials, nor is there any equivalent to this invasive power in PACE 1984. It is an offence under paragraph 14 to knowingly or recklessly make a false or misleading statement. By paragraph 13(4)(b), and in deference to Article 6, a statement in response to a requirement imposed by an order under this paragraph may be used in evidence against the maker only in a prosecution for an offense under paragraph 14, but not for other offenses.[188] There is no recorded use against a journalist.

The increasing usage of Schedule 5 reveals an official willingness to treat journalism as an available resource for the provision of journalistic information in pursuit of criminal justice or terrorism investigation purposes, but without much emphasis—beyond that stated in *ex parte Bright* in 2001—on other public interests such as a free and fearless press. The relative success of the tactic seems to have emboldened the police, especially in Northern Ireland, and so this second tactic of confrontation of journalism is now being rolled out on a global scale. This new front has become more feasible after 9/11, when the tendency to treat terrorism cases as "political offenses" and therefore not subject to international comity has tended to fade away, especially on the part of the U.S. authorities.[189] The point is illustrated by litigation around the Boston College tapes that will now be described.[190]

The "Belfast Project" began in 2001 as an oral history of the Northern Ireland Troubles. It was directed by journalist Ed Moloney, with the fieldwork being conducted by Wilson McArthur, for Loyalists, and Anthony McIntyre, for Republicans. The collection was to form a repository in the Burns Library at Boston College, thereby benefiting from full U.S. First Amendment rights and a degree of distance, so it

186. *Id.*

187. *See* Criminal Procedure Rules 2013, §§ 6.8, 6.13.

188. *See* Saunders v. United Kingdom, App No. 19187/91, 1996-VI; I.J.L v. United Kingdom, App Nos. 29522/95, 30056/96, 30574/96, 2000-IX.

189. For changing attitudes regarding extradition, *see* GEOFF GILBERT, TRANSNATIONAL FUGITIVE OFFENDERS IN INTERNATIONAL LAW: EXTRADITION AND OTHER MECHANISMS, ch. 6 (1998); CLIVE WALKER, TERRORISM AND THE LAW 253?296 (2011).

190. *See generally The Belfast Project, Boston College, and a Sealed Subpoena*, BCSN (2015), https://bostoncollegesubpoena.wordpress.com; Beth McMurtrie, *Secrets from Belfast*, THE CHRON. OF HIGHER EDUC. (Jan. 26, 2014), http://chronicle.com/interactives/belfast; Script of *The Good Friday Agreement*, CBS NEWS: 60 MINUTES (Apr. 5, 2015), http://www.cbsnews.com/news/gerry-adams-ireland-good-friday-agreement-scott-pelley-60-minutes/; Fraser Sampson, *"Whatever You Say. . .": The Case of the Boston College Tapes and How Confidentiality Agreements Cannot Put Relevant Data Beyond the Reach of Criminal Investigation*, POLICING (2015).

was thought, from the prying eyes of the British authorities. A key objective was to capture the views of live participants as a research resource and also as part of the eventual process of transitional justice through account-giving. Various former Loyalist and Republican paramilitaries gave candid interviews that chronicled their involvement in the Troubles. They were promised that the recordings and transcripts would only be made public after their deaths. Amongst those interviewed were David Ervine of the Progressive Unionist Party, and the former IRA commander Brendan Hughes—who died in 2007 and 2008 respectively—and some details were revealed in a book by Ed Moloney[191] and a television documentary broadcast by Raidió Teilifís Éireann in 2010.[192] It was probably naïve, arrogant, or both to suppose that the authorities would look the other way. Accordingly, the Police Service of Northern Ireland ("PSNI") took action, after hearing claims in the published statements of Hughes that the Sinn Féin leader, Gerry Adams, had been overall commander of the IRA's Belfast brigade and that he had been involved in a unit responsible for the "Disappeared"—those who were kidnapped, murdered and secretly buried by the IRA.[193] Though denied by Adams, another prominent Republican participant in the "Belfast Project," Dolours Price, who died in 2013, also gave information about her involvement in driving one of the "Disappeared," Jean McConville, to the place where the IRA murdered her in 1972.[194]

In March 2011, the PSNI began a legal bid in the U.S. to gain access to the interviews held by Boston College. Its investigation took the form of a request to the U.S. Department of Justice to initiate Mutual Legal Assistance Treaty proceedings by issuing a sealed subpoena for all materials relating to two interviews in the archive, those of Brendan Hughes and Dolours Price.[195] Boston College sought to quash the subpoena.[196] In August 2011, a second subpoena was served seeking "any and all interviews containing information about the abduction and death of Mrs. Jean McConville."[197] This was also opposed by the Belfast Project, including on the political argument that the Attorney General "should take cognisance of solemn promises made by the U.K. Government to the U.S. Senate that it would not reo-

191. ED MOLONEY, VOICES FROM THE GRAVE: TWO MEN'S WAR IN IRELAND (Faber & Faber eds., 2010).

192. Broadcasting Authority of Ireland and Radio Telefis Eireann, *Voices From The Grave,* BCSN (2010), https://bostoncollegesubpoena.wordpress.com/supporting-documents/voices-from-the-grave-documentary/.

193. *See* Northern Ireland (Location of Victims Remains) Act 1999, ch. 7, §§1–7; *see also* INDEPENDENT COMMISSION FOR THE LOCATION OF VICTIMS REMAINS, http://www.iclvr.ie/.

194. In August 2003, her remains were found by chance at Shelling Hill beach in County Louth. The IRA admitted her killing in 1999.

195. *See* Brief for the Petitioner in Supp,, Moloney & McIntyre v. Holder (D. Mass. 2011) (r).

196. *Id.*

197. *See* Brief for the Petitioner in Supp. (Second Subpoena), Moloney & McIntyre v. Holder (D. Mass. 2011) (No. 11-MC-91078).

pen issues addressed in the Belfast Agreement, or [ ] impede any further efforts to resolve the conflict in Northern Ireland."[198]

In December 2011, Judge William G. Young recognised that "subpoenae targeting confidential academic information deserve heightened scrutiny," but still ruled against both Boston College's motions to quash the subpoenas and Moloney and McIntyre's motion to intervene.[199] His proposal was to review the archives *in camera*, but this exercise was stayed pending an appeal to the U.S. Court of Appeals.[200] The First Circuit Court of Appeals gave judgment on the first subpoena on 6 July 2013, upholding Judge Young's ruling.[201] Any First Amendment challenge was rejected on grounds that there were no private rights under these international law arrangements and there was no judicial review of actions under a treaty. A stay was granted by the U.S. Supreme Court,[202] but certiorari was denied in 2013.[203] The First Circuit Court of Appeals ruled on Boston College's appeal and motions on 31 May, 2013. The court was critical of the breadth of the application and reduced the amount of material to be handed over from 85 interviews—out of 176 relevant interviews in total—to segments of 11 interviews.[204] But, at the same time, it crucially found that a promise of confidentiality by a researcher did not create a First Amendment bar.[205] The U.S. Attorney's application for a rehearing was denied.[206]

In early 2015, arrangements were made for sealed tapes to be sent to the Royal Courts of Justice in Belfast. Several legal consequences have ensued. First, Richard O'Rawe threatened to sue Boston College after it handed over parts of his interviews. He claimed breach of contract:

> Mr O'Rawe told of his career in the Provos to Boston College researchers on strict conditions contained in a 'donor contract' with the college. It stated that 'access to the tapes and transcripts shall be restricted until after my death except in those cases where I have provided prior written approval.' However, the contract didn't specify that the secrecy of the archive was limited under American law.[207]

198. *See* Intervenors'/Plaintiffs' Complaint for Declaratory Judgment, Writ of Mandamus and Injunctive Relief, Moloney & McIntyre v. Holder (D. Mass. 2011) (No. 11-MC-991078).

199. *See* United States v. Trustees of Boston College, 831 F. Supp. 2d 435, 455 (D. Mass. 2011).

200. *See* Brief for Appellant, United States v. Trustees of Boston College, 831 F. Supp. 2d 435 (D. Mass. 2011) (No. 12-1236).

201. *See generally* United States v. Moloney (*In re* Price), 685 F.3d 1 (1st Cir. 2012).

202. *See* Moloney v. United States, 133 S. Ct. 9 (2012).

203. *See* Moloney v. United States, 133 S. Ct. 1796 (2013).

204. *Compare* United States v. Trustees of Boston College, 718 F.3d 13 (1st Cir. 2013) *with* United States v. Trustees of Boston College, No. 11-91078-WGY, 2012 WL 194432 (D. Mass. 2012)

205. 718 F.3d at 20.

206. *See* United States v. Trustees of Boston College (*In re Price*), No. 12-1236 (1st Cir. 2013) (order denying petition for rehearing).

207. Liam Clarke, *Ex-IRA prisoner Richard O'Rawe: I'll sue Boston College for handing over tapes*, BELFAST TELEGRAPH (May 13, 2014), http://www.belfasttelegraph.co.uk/news/

Relevant materials were subsequently returned by Boston College to O'Rawe, who destroyed them, but some materials were still disclosed to the PSNI.[208]

Second, and even before the tapes had arrived, the police arrested Gerry Adams in May 2014 regarding his alleged role in the disappearance of Jean McConville. Adams was released without charge, and the then PSNI Chief Constable, Matt Baggott, rejected the "claim there were 'dark' elements opposed to the peace process behind his detention."[209] While Adams was not pursued, Ivor Bell was charged with IRA membership and aiding and abetting in the 1972 murder of Jean McConville, with part of the evidence being derived from the tapes.[210]

Third, and with the tapes now arriving on the doorstep of the United Kingdom jurisdiction, a number of interviewees began to consider their uncomfortable position. One such interviewee is Winston Rea, who was a member of the Red Hand Commando and who had provided testimony to the Belfast Project. Rea brought legal proceedings in Belfast to stop police from listening to the tapes. His counsel argued that prosecuting authorities were acting on a hunch rather than any firm knowledge that the tapes contain information relevant to any investigation and that the operative legislation, section 7(5) of the Crime (International Co-operation) Act 2003, breached Rea's right to privacy under the European Convention on Human Rights, article 8. After the application was rejected in the High Court, the PSNI officers travelled to Boston for the purpose of taking possession of the tapes. In February 27, 2015, the Northern Ireland Court of Appeal rejected the appeal.[211] The DPP argued that the standard to be established was simply that the evidence should be "for use" in the proceedings or investigation rather than that it must be of "substantial value."[212] Given that the legal test applied by the United States in such cases was that of "probable cause," the US Court of Appeals decision showed that sufficient grounds were made out for the material to be subpoenaed.[213] The DPP also argued that there was a duty to protect life under Article 2 of the European Convention on Human Rights to investigate murder

northern-ireland/exira-prisoner-richard-orawe-ill-sue-boston-college-for-handing-over-tapes-30267265.html.

208. Liam Clarke, *Boston College tapes: Archive that turned into a can of worms,* BELFAST TELEGRAPH (May 13, 2014), http://www.belfasttelegraph.co.uk/news/northern-ireland/boston-college-tapes-archive-that-turned-into-a-can-of-worms-30267260.html.

209. Henry McDonald, *Gerry Adams Arrest Defended by Northern Ireland Police Chief,* THE GUARDIAN (U.K.) (May 6, 2014). The quote is from Sinn Féin MP, and Deputy First Minister of Northern Ireland, Martin McGuinness.

210. *See* Alan Erwin, *Jean McConville: Former IRA man Ivor Bell charged with aiding and abetting murder is granted High Court bail,* BELFAST TELEGRAPH (Mar. 26, 2014), http://www.belfasttelegraph.co.uk/news/northern-ireland/jean-mcconville-former-ira-man-ivor-bell-charged-with-aiding-and-abetting-murder-is-granted-high-court-bail-30127724.html; *see also* Alan Erwin, *Lawyers for Jean Accused Bid to Get Case Thrown Out,* BELFAST TELEGRAPH (Nov. 20, 2015).

211. *See* In Rea (Winston Churchill) [2015] NICA (Civ) 8 (N. Ir.).

212. *Id.* at ¶¶ 10, 11.

213. *See id.* at ¶ 10.

in the interests of victims and the general public.[214] Lord Justice Coghlin accepted that the material could properly be subpoenaed in connection with the investigation stage and that, as a consequence, the PSNI do not have to identify specific aspects of the recordings which are relevant to the offences being investigated, other than they purport to be an account of terrorist activities carried out by the Red Hand Commando of which the PSNI hold prior information, as noted in the letter of request to American authorities indicating that Rea was an active member.[215] The standard specified in the 2003 Act for the grounds upon which the evidence is considered to be relevant for the purpose of a request for mutual assistance is that it is for "use in the proceedings or investigation."[216] Such evidence could not be of use if it was irrelevant but that was very far from reading into the 2003 Act any particular standard of relevance. Finally, any infringement of privacy would be covered by the exceptions in Article 8(2) to the European Convention on Human Rights. Though the judgment was decisively in their favour, before the PSNI could take away the tapes, the court ordered that the material remained sealed pending an appeal to the United Kingdom Supreme Court.[217] The Supreme Court declined to hear the appeal on May 19, 2015,[218] and the European Court of Human Rights also refused to grant an interim prohibition.[219] In June 2015, Lord Justice Coghlin declared that "[t]he time has come for us to lift the injunction and allow the materials to be examined by the police."[220]

In conclusion, this second round of intrusions into journalistic activities in order to support police and prosecution activities again have the tendencies to downplay the wider public interest attributes of journalism and also produce a chilling effect on the journalists and their sources. The only silver lining compared to the first round of intrusions, and the third round to follow, is that the courts tend to be heavily involved in the supervision of these interventions. As a result, while savings for journalistic purposes are often absent from the operative legal texts, the judges are alert to the issues under the European Convention on Human Rights, though, as shown in the Boston Project cases, the standards derived from that text are relatively weak, albeit that apparently stronger standards on free speech under the U.S. Constitution did not make much difference.

214. *See id.*

215. *See id.* at ¶ 14.

216. *Id.* at ¶ 22.

217. *Id.* at ¶ 25.

218. *Permission to appeal decisions by UK Supreme Court*, THE SUPREME COURT (May 19, 2015), https://www.supremecourt.uk/news/permission-to-appeal-decisions-19-may-2015.html.

219. Alan Erwin, *Boston College tapes: PSNI wins access to Winston "Winkie" Rea after court rejects final blocking bid*, BELFAST TELEGRAPH (June 6, 2015), http://www.belfasttelegraph.co.uk/news/northern-ireland/boston-college-tapes-psni-wins-access-to-winston-winkie-rea-after-court-rejects-final-blocking-bid-31280987.html.

220. *Id.*

IV. Duty to Inform Proactively

The foregoing mode of imposition upon journalism in the interests of counterterrorism demands action at the behest of the police. This third mode of imposition seeks to bypass the need for any police initiative. After all, why should journalists wait for a call if their information can save lives and if the police are unaware who possesses operative information in order to make a request? Better still to confer a general legal duty on everyone to inform without asking. Such a general duty would have particular purchase on journalism by recognising the forensic abilities of some journalists to obtain and analyse information that may sometimes exceed police capabilities in several ways. First, journalists may be able to carry out investigations not permissible by the police because of threshold requirements as to action or limitations on investigative techniques. Second, journalistic activity may be unencumbered by the finances of the police in an age of austerity.[221] Third, as illustrated by the Boston Project, some sources may be more willing to speak with journalists than with police officers. Consequently, the objective under this third heading is to make journalists duty-bound to serve up proactively information about terrorism and not simply act as potential but passive, and perhaps hostile, resources for search warrants or other forms of police-initiated investigation. The media must therefore turn themselves into self-tasking policing bodies.

The Terrorism Act 2000, section 38B, has conferred this insidious duty.[222] An offence is committed under section 38B(2) if a person, without reasonable excuse, fails to disclose information falling within section 38B(1), which is information which he knows or believes might be of material assistance in preventing the commission by another person of an act of terrorism, or in securing the apprehension, prosecution, or conviction of another person, in the United Kingdom, for an offence involving the commission, preparation, or instigation of an act of terrorism.[223] This special duty has existed in various guises since 1976, while in Northern Ireland it is also an offence under section 5 in the Criminal Law Act (Northern Ireland) 1967 to fail to give information known or believed likely to secure, or to be of material assistance in securing, the apprehension, prosecution or conviction of any person for an arrestable offence which has been committed.[224] Section 38B is different in that the information must relate to "terrorism" rather than an "arrestable offence" and may concern future as well as past activities. Nevertheless, the considerable overlap between section 38B and section

221. *See generally* Clive Walker & Andrew Staniforth, *The Amplification and Melding of Counter-Terrorism Agencies: From Security Services to Police and Back Again*, Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State 293 (Aniceto Masferrer & Clive Walker eds., 2013).

222. *See* Clive Walker, *Conscripting the Public in Terrorism Policing: Towards Safer Communities or a Police State?*, 2010 Crim. L. Rev. 441, 443; Clive Walker, Blackstone's Guide to The Anti-Terrorism Legislation 124–31 (2d ed. 2009).

223. *See id.*

224. Criminal Law Act 1967, c., § 18 (N. Ir.).

5(1) convinced the Baker Report to propose the repeal of section 5(1) as applied to "terrorist" offences.[225]

By section 38B(4), it is a defence for a person charged with an offence to prove a reasonable excuse for not making the disclosure. The defence of reasonable excuse will often relate to fears of reprisal or reaction going beyond the defence of duress.[226] Do journalists have a "reasonable excuse" to disregard this legal duty? A reporter may discover information about terrorism by interviewing a terrorist leader or by witnessing a paramilitary display. Arranging, attending, or reporting such events may implicate the journalist in various offences—especially attending a place of training under the Terrorism Act 2006, section 8—but section 38B can involve two further impacts. First, the offence contributes to a "chilling" effect on the reporting of terrorism. Correspondents can expect close attention from the police and hostility and special restrictions from their own superiors. Thus, coverage of Irish terrorism abounded with difficulties and was to some extent suppressed as "guilty secrets."[227] The second effect is the direct threat of prosecution where insufficient weight is given in section 38B to investigative journalism.[228] Such a threat occurred in 1979 and related to a BBC interview with an INLA representative and then the filming, but not the transmission, of an IRA roadblock in Carrickmore. Both events incurred the wrath of the Attorney-General, who issued a warning to the BBC on the 20 June 1980 that the incidents were of a nature "as constituting in principle offences . . . ."[229] Despite the threat, no prosecution has ensued.

There is no express exception for the media under section 38B, but the coercion or subsequent sanctioning of journalists is subject to article 10 of the European Convention on Human Rights, which applies two restraints. The more general is that the highest priority is given to the encouragement of journalism involving political speech.[230] The second aspect of protection is against legal incursions that demand the revelation of sensitive journalistic sources or confidences.[231]

In summary, despite the untrammelled breadth of its terms, some restraint has been applied in the usage of section 38B. It serves as a threat rather than the basis for making martyrs out of journalists who, on the evidence of the contempt cases arising from schedule 5 may not be easily convinced to divulge source material. However, the looming threat of prosecution certainly shifts the balance of power in the generally cooperative relations between media and police described earlier.

225. Sir George G. Baker, Review of the Operation of the Northern Ireland (Emergency Provisions) Act 1978 ¶ 253 (1984).

226. *See* R v. Sherif et al. [2008] EWCA (Crim) 2653 (Eng.).

227. Liz Curtis, Ireland: the Propaganda War 275 (1984).

228. *See* Walker, *supra* note 43 at 141–43.

229. The Times, August 2, 1980, at 2; *see also* Curtis, *supra* note 227, at 169–70.

230. *See* Castells v. Spain, App. No. 11798/85, 14 Eur. H.R. Rep. 445 (1992).

231. *See* Goodwin v. United Kingdom, App. No.17488/90, 22 Eur. H. R. 123, ¶ 39 (1996).

Section 38B was devised in the days of the IRA, when, geographically and tactically, a more confined conflict was played out between contestants who deeply understood each other. Now, the perception is of "new" terrorism,[232] which applies such global savagery that the old restraints of section 38B may also appear outmoded and weak. Another factor to take into account is the prolific storage and dissemination of data through the internet. As a result, there is increasing pressure on communication service providers both to impose restraints on their customers and also to keep the security authorities well informed about nefarious customer activities. Furthermore, these duties are very broadly pitched to apply not just to intelligence about offences or potential offences, but more generally to extremism and radicalization.

These extraordinary demands, which have not been imposed so much on other media, were made explicit in the United Kingdom in connection with the murder in Woolwich, South London, of Lee Rigby, a British Army soldier, on 22 May 2013. Those convicted of the murder, Michael Adebolajo and Michael Adebowale, drove their car at him and then attempted to behead him.[233] It emerged that Adebolajo had been detained under the Terrorism Act 2000, Schedule 7, after deportation on security grounds from Kenya in 2010 but that no further action was taken other than, allegedly, to recruit him as an informant.[234] Aside from these convictions, much of the focus of subsequent inquiries has concentrated on whether the murder could have been prevented, and two candidate organizations were put under the spotlight—the security agencies and the communications service providers. Perhaps surprisingly, much more blame has been attached to the latter than the former.[235]

The Prime Minister formed an Extremism Task Force after the killing of Lee Rigby, reported in late 2013.[236] One of its findings was that "[e]xtremist propaganda is too widely available, particularly online, and has a direct impact on radicalising individuals. The poisonous messages of extremists must not be allowed to drown out the voices of the moderate majority."[237] The Extremism Task Force agreed to:

- work with internet companies to restrict access to terrorist material online which is hosted overseas but illegal under UK law
- improve the process for public reporting of extremist content online

232. *See generally* BRYNJAR LIA, GLOBALISATION AND THE FUTURE OF TERRORISM (2005); PETER R. NEUMANN, OLD & NEW TERRORISM (2009).

233. *See* R v. Adebolajo [2014] EWCA (Crim) 2779 (Eng.); Sean O'Neill, *Muslim converts guilty of murdering Fusilier Lee Rigby*, THE TIMES (Dec. 19, 2013), http://www.thetimes.co.uk/tto/news/uk/crime/article3953546.ece.

234. *See Lee Rigby murder: What MI5 knew about Woolwich killers*, BBC (Nov. 25, 2014), http://www.bbc.com/news/uk-30196703.

235. *See, e.g.*, Claire Phipps, *Lee Rigby report: Facebook accused of failing to flag extremist messages—as it happened*, THE GUARDIAN (Nov. 26, 2014), http://www.theguardian.com/uk-news/live/2014/nov/25/lee-rigby-woolwich-inquiry-report-published-live-coverage.

236. *See* CABINET OFFICE, TACKLING EXTREMISM IN THE UK: REPORT FROM THE PRIME MINISTER'S TASK FORCE ON TACKING RADICALISATION AND EXTREMISM 1 (2013).

237. *Id.* at 3.

- work with the internet industry to help them in their continuing efforts to identify extremist content to include in family-friendly filters
- look at using existing powers to exclude from the UK those who post extremist material online who are based overseas.[238]

Next, the Intelligence and Security Committee's *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* found that the security services investigated these individuals on several occasions, but nothing immediately threatening to life had turned up.[239] The agencies knew of their extremism and wanted to use them as informants, especially as they could be pressured as a result of involvement in drug dealing. In short, the agencies acted properly within the resources available—a finding similar to the inquiries into the July 7, 2005 London bombings,[240] even though it was clear that the Woolwich pair were of much higher profile than the 7/7 group. However, the Intelligence and Security Committee does criticize the security agencies in some respects: stronger alarm bells should ring when an individual recurrently becomes of interest, and the Security Intelligence Service must be more proactive and take a greater interest in the activities of cooperating foreign agencies, including allegations of misconduct.[241] Yet, the most trenchant criticism is made of the failure of internet companies, especially the unnamed Facebook, for their failure to be more forthcoming in terms of alerting the authorities.[242]

Much of the subsequent media and political attention concentrated on the behaviour of Facebook. Several of Michael Adebowale's multiple social media internet accounts were closed proactively by Facebook and without official request because the accounts "hit triggers . . . related to their criteria for closing things down on the basis of terrorist content."[243] Facebook also learned, on completion of a retrospective review of all his 11 accounts,[244] that Adebowale had discussed "in the most explicit and emotive manner" over Facebook's instant messaging service his desire to murder a soldier.[245] The ISC was nevertheless critical of monitoring procedures by CSPs,[246] though serial investigations by the Security Service were excused as sufficiently thorough, especially because, as pointed out by GCHQ, true intent can be

238. *Id.* at 3.

239. *See* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, REPORT ON THE INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY, 2014–15, HC 795, at 165–72 [hereinafter ISC REPORT].

240. *See* HOUSE OF COMMONS, REPORT OF THE OFFICIAL ACCOUNT OF THE BOMBINGS IN LONDON ON 7TH JULY 2005, 2005–06, HC 1087, at 26. *See generally* INTELLIGENCE AND SECURITY COMMITTEE, COULD 7/7 HAVE BEEN PREVENTED?, 2009, Cm. 7617.

241. 25 Nov. 2914 Parl Deb HC (6th ser.) (2014) col. 747 (UK), http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm141125/debtext/141125-0001.htm.

242. Sean O'Neill et al., *Rigby killer's Facebook plot*, THE TIMES (Nov. 26, 2014), http://www.thetimes.co.uk/tto/technology/internet/article4278479.ece.

243. ISC REPORT, *supra* note 239, at 128.

244. *See id.* at 130.

245. *Id.* at 129.

246. *See id.*

very difficult to discern from online communications.[247] Thus, even if Facebook had passed on the offending messages to the security agencies, any reaction by them was far from assured and had been eschewed on several previous occasions. Though Facebook was not wholly forthcoming, their default raises two further jurisdictional issues. One is that their activities, based in the US, are overseen by the US security agencies; thus the Intelligence and Security Committee rather coyly referred to a "partner" foreign agency, but without asking whether it knew what was said on Facebook about killing a soldier and whether it consciously failed to pass on that information to the British agencies.[248] A second jurisdictional point is that even in the case of clear default, any proactive legal duty would have limited impact on a company based in the United States and any attempt to subpoena information would be laborious, as shown by the Boston Project case.

Taking up the last point, Sir Nigel Sheinwald was subsequently appointed as Special Envoy on intelligence and law enforcement data sharing in order to secure better transatlantic data sharing.[249] His report[250] included some achievements from his dialogues in the United States, which had helped to secure that the major social media internet companies will act on the most urgent requests by treating selected UK policing and security agencies as "trusted flaggers" so as to remove materials, though "cooperation remains incomplete."[251] Sheinwald's longer-term proposals are built around both greater data sharing between government agencies, though there is already very strong cooperation between the UK and US through the "Five Eyes" arrangements,[252] and reform to mutual legal assistance treaties[253] so that they

247. *See id.* at 130–32.

248. *See id.* at 131.

249. *See* Press Release, Cabinet Office et al., Sir Nigel Sheinwald Appointed Special Envoy on Intelligence and Law Enforcement Data Sharing (Sept. 19, 2014), https://www.gov.uk/government/news/sir-nigel-sheinwald-appointed-special-envoy-on-intelligence-and-law-enforcement-data-sharing.

250. SIR NIGEL SHEINWALD, SUMMARY OF THE WORK OF THE PRIME MINISTER'S SPECIAL ENVOY ON INTELLIGENCE AND LAW ENFORCEMENT DATA SHARING (2015).

251. *Id.*; *see also* David Barrett, *Google to deliver wrong 'top' search results to would-be jihadis*, TELEGRAPH (Feb. 2, 2016), http://www.telegraph.co.uk/technology/google/12136765/Google-to-deliver-wrong-search-results-to-would-be-jihadis.html; Hugh Handeyside, *Social Media Companies Should Decline the Government's Invitation to Join the National Security State*, JUST SECURITY (Jan. 12, 2016), https://www.justsecurity.org/28755/social-media-companies-decline-governments-invitation-join-national-security-state/; Jonathan Zittrain, *A Few Keystrokes Could Solve the Crime. Would You Press Enter?*, JUST SECURITY (Jan. 12, 2016), https://www.justsecurity.org/28752/keystrokes-solve-crime-press-enter/.

252. British-US Communication Intelligence Agreement, U.K.-U.S., Mar. 5, 1946, http://discovery.nationalarchives.gov.uk/details/r/C11536914; British-U.S. Communication Intelligence Agreement, U.K.-U.S. (June 26, 1951), https://www.nsa.gov/public_info/_files/ukusa/ukusa_comint_agree.pdf; British-U.S. Communication Intelligence Agreement, U.K.-U.S., May 10, 1955, http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf. *See* Sir Stephen Lander, *International Intelligence Cooperation: An Inside Perspective*, 17 CAMBRIDGE REV. INT'L AFF. 481, 491 (2004); Patrick F. Walsh & Seumas Miller, *Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden*, 31 INTELLIGENCE & NAT'L SECURITY 345 (2015).

253. *See* Council Decision 2009/820/CFSP, 2009 O.J. (L 291) 40; Instrument as Contemplated by Article 3 (2) of the Agreement on Mutual Legal Assistance Between the

become less "slow, unresponsive (it can take up to nine months for information to be returned) and bureaucratic (it currently involves hard copies of legal documents being couriered across the Atlantic through numerous intermediary bodies)."[254] Some of the envisaged changes are merely technical and bureaucratic. Much more ambitious is the proposal by Sheinwald for a new international framework about data sharing on counter-terrorism. However, previous disputes over trans-Atlantic data sharing in regard to terrorism indicate the extreme difficulties of reaching such an agreement if it is to go beyond the relative informality of the existing "Five Eyes" arrangements.[255]

Putting aside other relevant issues around data privacy, accountability for surveillance, the duty of care to users, and the economic efficiency, were social media companies to be legally obliged to proactively monitor and share all postings of a violent extremist nature with the security authorities, both would be deluged with information and rendered unable to function on an economic basis. Yet, the allure of blaming a foreign internet company rather than home security agencies for failing to avert atrocities seems to have been hard to resist in the U.K. even though it is clear that the Woolwich murder revealed a failure of assessment, perhaps understandable and excusable, rather than any crucial lack of information.[256]

United States of America and the European Union signed 25 June 2003, as to the Application of the Treaty Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, U.K.-U.S., Jan. 6, 2004. *See generally* Sarah Cortes, *MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance*, 22 RICH. J. L. & TECH. 1 (2015); ANDREW K. WOODS, GLOB. NETWORK INITIATIVE, DATA BEYOND BORDERS (2015).

254. SHEINWALD, *supra* note 250, at 2.

255. *See* Agreement Between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program, Eur. Union-U.S., July 27, 2010, 2010 O.J. (L 195) 5 (a previous version having been rejected by the European Parliament); Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security 13668/08, Oct. 8, 2006, Eur. Union-U.S., 2006 O.J. (L 298) 29; Annexes to Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security 11304/07, June 28, 2007 (a previous version being successfully challenged in Joined Cases C-317/04 & C-318/04, Parliament v. Council and Commission 2006 E.C.R. I-04721); Commission Decision 2000/520/EC of 26 July 2000 On the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce 2000 O.J. (L 215) 7 (EU) (as successfully challenged in Case C-362/14, Schrems v. Data Prot. Comm'r). *See generally*, Francesca Bignami & Giorgio Resh, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 LAW & CONTEMP. PROBS. 101 (2015).

256. *But see* Hugo Rifkind, *Google vs governments—let the new battle for free speech begin*, THE SPECTATOR (Nov. 29, 2014), http://www.spectator.co.uk/2014/11/nerds-spies-and-terrorists-the-online-battle-for-freedom-of-the-press/; James Forsyth, *The technology giants are breathtakingly irresponsible about terrorism*, THE SPECTATOR (Nov. 29, 2014), http://www.spectator.co.uk/2014/11/the-technology-giants-are-breaktakingly-irresponsible-about-terrorism/.

The head of the U.K. Security Service, Andrew Parker, kept up the pressure in his first public speech in early January, 2015 by emphasizing the need for powers to access and intercept communications.[257] His call was soon followed by the Government's reply to the Intelligence and Security Committee, which was adamant that:

> Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks. . . . [W]e are also pushing CSPs to take stronger, faster and further action to combat the use of their services by terrorists, criminals and their supporters. They are committed to measures that make it easier for their users and the authorities to report terrorist and extremist propaganda. We will build on this to encourage companies to work together to produce industry standards for the identification, removal and referral of terrorist activity.[258]

By contrast, the government expressed itself "confident that MI5 prioritises available resources and deploys them proportionately to the level of risk represented and as necessary to satisfactorily mitigate the risk, based on the information known at the time."[259] Yet it seems, by contrast, that CSPs are expected to perform to a higher duty of care with no margin for error or discretion: "Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks."[260] A more realistic understanding is that even with extensive criminal offences, intrusion into free speech activities, the appointment of extra staff, and extra funding, not all terrorism will be averted. It is unrealistic to expect internet companies to act as better all-seeing and all-doing state spies than the security agencies themselves.

Despite these doubts, the tactic of imposing a duty to inform proactively seems no longer to be a British obsession but is one that is seeping into the U.S. psyche. Though not backed by criminal sanction, such as in section 38B of the Terrorism Act 2000,[261] the U.S. Congress passed the Cybersecurity Information Sharing Act at the end of 2015 to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes."[262] The Act permits the sharing of internet traffic information between the U.S. government and technology and manufacturing companies.[263] As

257. *See* Andrew Parker, Director General, Security Service, Address to the Royal United Services Institute at Thames House: Terrorism, Technology and Oversight (Jan. 8, 2015).

258. CABINET OFFICE, GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT REPORT ON INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY 5–6 (2015).

259. *Id.* at 7.

260. *Id.* at 5.

261. Terrorism Act 2000, c. 11, § 38B (U.K.).

262. S. 754, 114th Cong. (2015) (enacted). The Act forms Division N of the Military Construction and Veterans Affairs and Related Agencies Appropriations Act, 2016. *See* Consolidated Appropriations Act, 2016, Division N, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

263. *See* S. 754, 114th Cong. §§ 103, 105 (2015)

mentioned, there is no compulsion to do so, but the sharing of personal information is authorised as a function of government, with the Department of Homeland Security providing the conduit. Furthermore, personal information may be used as evidence for crimes involving any "terrorist act or a use of a weapon of mass destruction" (under section 105(d)(5)(A)(iv)).[264] One Bill proposed around the same time, the Combat Terrorist Use of Social Media Act of 2015, would have required analysis of how terrorists and terrorist organizations are using social media.[265] Another Bill, Requiring Reporting of Online Terrorist Activity Act of 2015, went much further by demanding that

> Whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any terrorist activity, including the facts or circumstances described in subsection (c), shall, as soon as reasonably possible, provide to the appropriate authorities the facts or circumstances of the alleged terrorist activities.[266]

However, no sanction was specified for default, and Congress has not enacted either Bill.

V. Conclusions

The modes of treating journalists either as akin to terrorists or in some cases as akin to police officers are not new. The history of demands, threats, and prosecutions extends over several decades. But confrontational stances seem to be growing more prevalent and more insistent. Factors that might explain this trend have broadly been identified as reflecting two vectors. One relates to the perceived nature of terrorism. The "new" terrorism is seen as more threatening and therefore demands greater societal mobilization and lower tolerance to risk. As a result, counterterrorism is allowed to transcend other values, including the expressive rights of journalists and the privacy rights of their sources. The other vector relates to the perceived nature of the journalism and the media. The official perception seems to be that the media has grown more powerful as private actors and should therefore be viewed as more potentially threatening to the public interests of counter-terrorism.

Assuming that these trends of hostility to journalism are occurring, what should be the reactions? Some international law authorities have expressed concern. In particular, the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to

264. *Id.* at § 105(d)(5)(A)(iv).
265. H.R. 3654, 114th Cong. (2015).
266. S. 2372, 114th Cong. § 2(a) (2015).

Information issued a *Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation* in 2008 which proposed that:

> The definition of terrorism, at least as it applies in the context of restrictions on freedom of expression, should be restricted to violent crimes that are designed to advance an ideological, religious, political or organised criminal cause and to influence public authorities by inflicting terror on the public.
>
> The criminalisation of speech relating to terrorism should be restricted to instances of intentional incitement to terrorism, understood as a direct call to engage in terrorism which is directly responsible for increasing the likelihood of a terrorist act occurring, or to actual participation in terrorist acts (for example by directing them). Vague notions such as providing communications support to terrorism or extremism, the 'glorification' or 'promotion' of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised.
>
> The role of the media as a key vehicle for realising freedom of expression and for informing the public should be respected in anti-terrorism and anti-extremism laws. The public has a right to know about the perpetration of acts of terrorism, or attempts thereat, and the media should not be penalised for providing such information.
>
> Normal rules on the protection of confidentiality of journalists' sources of information—including that this should be overridden only by court order on the basis that access to the source is necessary to protect an overriding public interest or private right that cannot be protected by other means—should apply in the context of anti-terrorist actions as at other times.[267]

A more recent statement of devotion is the European Union's *Human Rights Guidelines on Freedom of Expression.*[268] Paragraph 31 states "States should protect by law the right of journalists not to disclose their sources in order to ensure that journalists can report on matters in the public interest without their sources fearing retribution."[269] Similar sentiments are made in the paragraph regarding information and communication technologies.[270] Annex 1 recognises that "the protection of national security can be misused to the detriment of freedom of expression," and so "States must take care to ensure that anti-terrorism laws, treason laws or similar provisions relating to national security (state secrets laws, sedition laws, etc.) are crafted and applied in a man-

267. Organization of American States, *Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation* (Dec. 9, 2008), http://www.oas.org/en/iachr/expression/showarticle.asp?artID=735&lID=1.

268. Council of the European Union, *EU Human Rights Guidelines on Freedom of Expression Online and Offline* (May 12, 2014).

269. *Id.* at 7.

270. *Id.* at 9.

ner that is in conformity with their obligations under international human rights law."[271]

By contrast to this soft law, harder-edged international law, such as the already mentioned UN Security Resolution 2178,[272] has pushed in the opposite direction, and ideas around offering more protection to journalists, including in conflict zones, have not been delivered.[273]

Turning to domestic safeguards, broad constitutional statements of values, such as freedom of expression, have the virtues of coverage and importance, but they also reflect limits. Even the First Amendment to the United States Constitution did not forbid the rendition of the Boston Project tapes and has also allowed the enforcement of material support offences.[274] Likewise, Article 10 of the European Convention on Human Rights has proven relatively weak when challenged by operational requirements of counter terrorism. Within the Human Rights Act 1998, there is the further boost to freedom of expression given by section 12 which was enacted to "tip the balance" in favour of expression.[275] However, in *Douglas v. Hello! Ltd.*,[276] section 12(4) was not interpreted as according to Article 10 as a presumptive priority over other rights.[277] Despite its uncertain impacts, section 12(4) has been used as a precedent in the Counter Terrorism and Security Act 2015, section 31, for giving a special boost to freedom of speech in the application of the "Prevent" duty (countering violent extremism) to universities.[278]

In the light of these experiences, it would seem that if freedom of expression is to be better safeguarded against counter terrorism, more

271. *Id.* at 16.

272. *See* U.N. Secretary General, *Human Rights in Armed Conflicts: Protection of Journalists Engaged in Dangerous Missions in Areas of Armed Conflict*, U.N. Doc. A/10147 (Aug. 1, 1975).

273. *See generally* Emily Crawford & Kayt Davies, *The International Protection of Journalists in Times of Armed Conflict: The Campaign for a Press Emblem*, 32 WIS. INT'L L.J. 1 (2014); Laura M.J. Fournier, *The Protection of Journalists in Armed Conflict* (2013–14) (unpublished Master thesis of the 'Master of Laws,' Ghent University) (on file with Ghent University Law School).

274. *See* 18 U.S.C. § 2339A (1994); 18 U.S.C. § 2339B (1996). *See, e.g.*, United States v. Lakhani, 480 F.3d 171 (3d Cir. 2007); United States v. Iqbal, No. 1:06-cr-01054 (S.D.N.Y. Apr. 27, 2009); Holder v. Humanitarian Law Project, 561 U.S. 1 (2010). *See generally* Peter Margulies, *Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech*, 63 HASTINGS L.J. 455 (2012); Adam Tomkins, *Criminalizing Support for Terrorism: A Comparative Perspective*, 6 DUKE J. CONST. L. & PUB. POL'Y 81 (2011); David Cole, *The First Amendment's Borders: The Place of* Holder v. Humanitarian Law Project *in First Amendment Doctrine*, 6 HARV. L. & PUB. POL'Y REV. 147 (2012); George D. Brown, *Notes on a Terrorism Trial—Preventive Prosecution, "Material Support" and The Role of the Judge After* United States v. Mehanna, 4 HARV. NAT'L SEC. J 1 (2012); Nikolas Abel, Note, United States v. Mehanna, *The First Amendment, and Material Support in the War on Terror*, 54 B.C. L. REV. 711 (2013); Emily Goldberg Knox, Note, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295 (2014).

275. *See* RICHARD CLAYTON & HUGH TOMLINSON, THE LAW OF HUMAN RIGHTS § 15.22 (2d ed. 2009).

276. Douglas v. Hello! Ltd. [2000] EWCA (Civ) 353, [2001] Q.B. 967 (Eng.).

277. *See id.* at 136.

278. *See also* J Blackbourn & Clive Walker, *Interdiction and Indoctrination: The Counter-Terrorism and Security Act 2015*, 79 MODERN L. REV. 840 (2016).

specific and stronger savings must be inserted into specific policing and court powers. One precedent is the saving for excluded and special procedure journalistic material under sections 11, 13, and 14 of PACE.[279] The same idea is now being advanced in relation in the interception of communications data under the Regulation of Interception of Communications Act 2000.[280] Even the Home Office's revised Code of Practice on Schedule 7 makes significant concessions to journalistic materials.[281] Special savings of this kind may, in practical terms, require a higher threshold for intervention against journalistic materials and/or may require a stricter level of authorization or supervision of the intervention—such as a judicial warrant. The same devices could be applied more widely in counter-terrorism legislation and on a firmer basis than by means of a code of practice.

For the foreseeable future, the value of counter-terrorism will continue to be played as a trump card against journalistic data and the interests of free expression and free information in many societies. The trends now impinging on journalistic activities with reference to counter-terrorism seem set to strengthen for now.

279. Police and Criminal Evidence Act 1984, c. 60, §§ 11, 13, & 14 (UK).

280. *See* INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE, IOCCO INQUIRY INTO THE USE OF CHAPTER 2 OF PART 1 OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) TO IDENTIFY JOURNALISTIC SOURCES (2015).

281. *See* HOME OFFICE, EXAMINING OFFICERS AND REVIEW OFFICES UNDER SCHEDULE 7 TO THE TERRORISM ACT 2000: CODE OF PRACTICE (2014).